

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Legal Challenges and Consumer Protection in India's Digital Payment Ecosystem: A Comparative Study of UPI Regulations and Global Frameworks

POORVAJA G¹

ABSTRACT

This research paper takes stock of the legal battles and consumer protection regimes that shape it uniquely vis-a-vis emerging global regulatory paradigms to assess the prospects of India's Unified Payments Interface (UPI) ecosystem. The rapid growth of payment systems in India, especially UPI (Unified Payment Interface) that started by making transactions as low as Re 1 possible, processed upwards of over 18 billion monthly in total between April - September period of this year; therefore needs solutions to balance out innovations with safeguards for consumer against misuse. The study examines three key questions: To what extent does the current legal architecture in India provide protection to consumers of digital payments? What can be learnt from recent developments in regulation in the United Kingdom, Singapore and the European Union? And how should Indian law develop to balance emerging conflicts between data protection, liability for fraud and regulation of payment systems?

This study uses a doctrinal legal approach, reviewing primary sources such as the Payment and Settlement Systems Act 2007, the Digital Personal Data Protection Act 2023, RBI circulars and master directions, as well as international instruments like the United Kingdom's APP Fraud Mandatory Reimbursement Framework and Singapore's Shared Responsibility Framework. Much of the insight comes from specific opinions on wide gaps in India's consumer protection regime, such as the allocation of liability for authorised push payment fraud, the conflict between data protection based on consent and payments without friction, and a lack of enforcement despite rule-making. Supports strengthening remedies, including a statutory compensation system for low-value fraudulent transactions. These proposals aim to position Indian law at the forefront of digital payment governance while ensuring that consumer protection keeps pace with technological innovation.

Keywords: *Unified Payments Interface, Consumer Protection, Digital Payments, Data Protection, Authorised Push Payment Fraud, Comparative Law, Financial Regulation*

¹ Author is a Student at Amity Law School, Noida, India.

I. INTRODUCTION

A. The Digital Payment Revolution in India

The Indian digital ecosphere underwent a massive evolution in the recent era. A major contribution to this revolution was made by the introduction of the Unified Payment Interface by the National Payments Corporation of India (NPCI hereafter) transforming the framework for transactions in India. The transactions are made via a QR Code and are accepted in all facets of our remunerative life. India entered the global pedestal when the UPI payment framework witnessed over 18 billion transactions in one month in the beginning of 2025.

The attributes that made these transactions supreme such as the promptness of payments and versatility with respect to operations also exposed them to several risks and susceptibility. Official Reports from the Home Affairs Ministry confirmed that the cases of embezzlement and financial misconduct saw a significant rise in 2023. Over 13 lakh cases were registered in the onset of 2023 as opposed to 7 lakhs, the figure before the flourishing of the modern digital system. A result of a survey proved that a lot of cases of financial fraud go unreported even though one in five Indian families encounter it. This data reflects the lacuna between innovative development of the UPI framework and creation of solid laws protecting the breach of it.

The creation of regulations catering to digital payments has been fragmented and of a reactive nature. Legislations such as the Payment and Settlement Systems Act 2007, the Circulars of RBI, guidelines of NPCI and the Digital Personal Data Protection Act 2023 (DPDP Act) together create a base structure for governing of the UPI transactions. Despite the presence and enforcement of these acts, an array of questions remained unanswered. Such as, upon whom will the burden of loss lie when a consumer is deceived into sanctioning a dishonest transaction? What is the role of the intermediary used for the payment transaction towards the security of its customers and what authority would be responsible for their supervision?

India is not the only country struggling to answer these questions. These are also the common concerns of all the nations participating in the creating of a digitized payment system. Countries such as the United Kingdom created initiatives such as Authorized Push Payment Fraud Mandatory Reimbursement Framework.²

This study is done with an intention to understand India's blueprint to engineer the digital payment system as it enters the Global trend of digital innovation with various countries. By understanding the current laws of other countries, recognizing gaps and improvements in our regulations and

² Jyothi, M.N., 2025. *An Evaluation of the Legal Framework of Electronic Banking with Special Reference to Data Protection and Cyber Security in India* (Doctoral dissertation, Alliance University (India)).

amending them in a way they are suitable for the Indian audience is one of the main objectives of this paper. The ultimate goal however, is to think of long-term solutions and methodologies to strengthen the laws governing consumer protecting and minimize vulnerabilities.

II. CONCEPTUAL FRAMEWORK OF DIGITAL PAYMENTS AND CONSUMER PROTECTION

A. Introduction

The combining of digitization and financial management system of India resulting in the creation of a UPI system has been a revolutionary aspect in creating a strong and structured economy. The UPI system Was created by creating a blend of technology financial systems, regulations and legislations in a way that enabled Users to make prompt payments and ease of transactions stop the creation of the system was not easy as there was an interplay of various fields involved. A key element that had to be kept in mind Was the protection of consumers and the prevention of risks that have the potential of arising from these transactions such as cyber fraud, data breaches to name a few.³

The aim of this chapter is to create a base framework by doing a detailed study on the repercussions of digitising transactions and their effects on the protection of the consumers. This chapter explores the current financial management system, the features of the UPI system and their nature and the scope of the consumer protection laws of India to accommodate a massive intervention of technology in the already existing transactions.

B. Concept and Nature of Digital Payment Systems

A digital payment transaction created with an intention to ease the flow of commercial transaction by allowing the transfer of monetary value electronically without the involvement of any tangible asset. These can take the form of net banking credit card transactions and platforms that allow instant payments. The UPI system stands apart due its highlights such as the removal of the requirement of tangible assets, speed and removal of need of physical presence to make the payments.

Focusing on the legal aspects of these transactions, the introduction of UPI payments remodels the applicability of evidence and contract laws. The Information Technology Law of India Recognises electronic records as legally valid instruments. Providence just Section 4 and 5 of the Information Technology Act cater to granting legal validation to digitised documents and E-Signatures. The introduction of these provisions was done to ensure that these transactions meet the standards of the traditional contracts and agreements. This inclusion facilitated the initiation of digital transactions in

³ Malik, R., Gahlyan, A. and Singh, N., 2025. A Comparative Study of UPI Digital Payment Adoption and Its Economic Impact in Rural and Urban India. *Anjali and Singh, Neha and Singh, Neha, A Comparative Study of UPI Digital Payment Adoption and Its Economic Impact in Rural and Urban India (October 27, 2025)*.

India.

These payment systems are not restricted to financial management agencies in India. They include banks service providers stakeholders and many intermediaries that conduct businesses involving transfer of payments. These associations are monitored by formal method suggest contracts regulations and legislations. Since many parties depend on these financial systems for a seamless transaction, it needs to be ensured that the legal structure and the technological structure can handle the wait of such complex transactions.⁴

C. Theoretical Foundations of Financial Regulation

The regulation of finances is done in the form of theories and the aim at improving failures in the market and prioritising the interest of the public initially the introduction of digital payment systems into the market can create vulnerabilities in terms of information assimilation, system exposure and other external issues. The role of regulatory authorities is to keep these risks under control and create contingency plans to solve these problems when they appear at face value.

The consumers may not have the technical knowledge too understand the risks with respect to security and data protection. So, theorising the regulations to simplify the list of rights that a consumer can invoke in cases of breach is extremely important. These regulations ensure that the operators and the service providers conduct smooth transactions adhere to all the provisions of the relevant acts. Another hindrance that can be created is to ensure that there is no financial instability in the payment systems when there is an imbalance in the economy. To prevent this, authorities ensure constant supervision of the market and the economy and its impact on the digital payable system. An important observation made from this is that for any activity that is done for public good, good governance and regulations are primary.

D. Legal Concept of Consumer Protection in Digital Transactions

Consumer protection laws Combine certain principles of traditional law Such as tort law and contract law when included under the purview of digital payment transactions. Consumers come and contact with these digitised platforms by accepting some standard contractual conditions that can sometimes include technical intricate terms. To ensure that there is a balance between the powers of the service providers and the powers of the consumers the law intervenes.

The Consumer Protection Act 2019 officer broad definition of consumers. One aspect that it covers under the definition of consumers is the users of e commerce platforms. It recognises the necessity to provide redressal when there is a deficiency in service by the service providers Section 2(11) of

⁴ Prasad, A., 2025. Regulatory Challenges in the Era of Digital Banking and Fintech: A Framework for India's Evolving Financial Ecosystem.

the Consumer Protection Act addresses the non-performance of services, especially when there is a contractual obligation. This provision with respect to payment in digital platforms will take the form of incomplete processing of transactions, breach of security information and dispute resolution.⁵

The consumer protection law ensures that there is transparency in terms of any fees involved, security measures undertaken, terms of service etc. The law-making authorities ensure that thorough investigation is done when violation is suspected and compensation is provided to the victims. The violations can take the form of misrepresentations, unauthorised access etc.

E. Risk Dimensions in Digital Payment Ecosystems

Risks can be classified into many types. With respect to UPI systems risks can be mainly classified into 3 types. These include operational risk, legal risks, and cyber security risks. Operational risks in terms of digital payment systems can take the form of failures of system or malfunctioning of transactions and disruptions created in the technology. Cyber security risks include fraudulent transactions access of information without authorization and leakage of data. Legal risks include loopholes that are yet to be decided or are uncertain which can be in terms of contracts, evidence and regulations.

Some provisions in the information technology Act 2000 were introduced to highlight the responsibilities of service providers. One such provision list section 43 A of the information technology act, 2000. This provision creates a liability in the form of compensation when there is a breach in implementing security practices by the operator. Provisions such as these enhance the investment in the innovation of cyber security and data protection. The information technology act is not restricted to civil damages alone. Section 66 of the act allows criminal sanctions in the case of access without authorization and fraudulent transactions.

These regulations and legislations act as a checklist to ensure that the technological innovation is conducted while meeting the legal requirements. Mechanisms that act as grievance mechanisms in case an incident with respect to breach of regulations is done should be enforced for immediate redressal. The main aim of such provisions is to reduce the susceptibility of the consumers as well as the operators.

F. Principles of Liability and Accountability

While the introduction of digital payments was done, an important component of deciding the liability that will arise from various disputes that may possibly occur with respect to intermediaries and consumers had to be studied and compiled. The main aim of deciding the liability what's to

⁵ Pereira, R.A., 2025. Comparative Study of Online Payment versus Offline (Traditional) Payment with Emphasis on UPI in India and Changing Payment Regulations (Doctoral dissertation, Dublin, National College of Ireland).

answer a significant question that is with whom the liability will lie in case of unauthorised transactions. This part a debate as in some situations both the service providers and the consumers were in a vulnerable position. Some countries undertook a modern approach of implementing shared responsibility between the service providers and the consumers.

The central bank and the payment and settlement systems Act 2007 created directions that stated that the operators responsible for governing these payment transactions must ensure that system is secure and a structured grievance mechanism system is set up. The consumer protection laws rely on judiciary for the adjudication of disputes with respect to vulnerabilities created out of these digital systems. Section 79 of the information technology Act 2000 introduced the necessity of conducting due diligence on intermediaries that use these digital payment platforms. The current mechanism tries to ensure that the people who take advantage of the vulnerabilities of consumers are held liable.⁶

G. Role of Technology in Shaping Legal Norms

The existence of current technology helps in identifying the basic legal protection measures that need to be undertaken while the mechanism of digital payments is structured. This includes concepts such as encryption, data analysis, authentication etc. So, the legal frameworks miss and sure that these basic benchmarks are fulfilled first. The guidelines with respect to progress and innovation and technology are often updated by the regulatory authorities.

The inclusion of the provisions recognising digital signatures and digital records was a landmark move that demonstrated the government's willingness to replace the traditional models governing transactions with the fast paced technologically advanced means. Thus, the intersection that the introduction of UPI system created between technology and law was revolutionary.

H. International Perspectives on Digital Payment Regulation

One of the main characteristics of digital payments is that it removes jurisdictional barriers and allows international transactions. When international transactions are involved, it is necessary to understand the regulatory mechanisms that other countries implement in order to develop and protect the growth of innovation in a secure manner. A common point for all nations in terms of digital transactions and innovations is to strengthen data protection and create strong consumer protection law that will accommodate all the loopholes that the introduction of digital payments can potentially bring.

⁶ Agbelade, O., 2023. A Comparative Analysis of Financial Technology (Fintech) Legal Framework: Blockchain, Mobile Payment Solutions & Data Protection As Special Case Study. Mobile Payment Solutions & Data Protection As Special Case Study (December 20, 2023).

To accomplish this countries often cooperate and exchange their practices and standards with each other in order to create an integrated system devoid of any loopholes. By participating in these global transactions countries together address the potential risks that can arise from these transactions and acknowledge the existence of cybercrimes that will create vulnerabilities for the consumers and suggest a framework to minimise or deal with the consequences.

I. Ethical and Societal Dimensions of Digital Payments

In today's era data protection privacy inequity are given immense importance as add country witnessed the various vulnerabilities that can be created if ignored. So, it was important to ensure data these digital modes of payment fulfill the ethical and societal standards of protection of data apart from the legal standards. The processing of data and participation in the transactions by an individual without the interference of any middleman or intermediary created a sense of privacy and confidentiality. What needs to be ensured that the legislation and regulations keep up with the advancements and technology Android prevent innovation from creating social and ethical challenges. As the technology witnesses advancements social responsibility and ethical governance need to raise their standards in parallel as well.

III. REGULATION OF UPI AND MOBILE WALLETS IN INDIA

The rampant use of the digital payment systems in all sectors for various transactions raises an important question of the difference between mobile wallets and UPI's which are classified under the same umbrella by the RBI under the title of Prepaid Payment Instruments (PPI). Both these systems have overlapping provisions, regulations and implications. However, there is a distinction between the terms and their meaning.

There are four main authorities governing the Digital Payment Systems in India. The Reserve Bank of India is responsible for governing the authorization of PPIs, regulation of KYC, licensing of banks and sets up cyber security measures. The National Payments Corporation of India also known as the system provider by the Reserve Bank of India, undertakes responsibilities such as the operation of the UPI frameworks, issues circulars with respect to the Digital Payment Systems in India. The third authority linked to the UPI systems are the banks. All transactions occur via the banks. The money wallets and the UPI payments are associated with banking transactions. Finally, applications such as Google Pay, BharatPe etc., that are governed under the agreement called TRAP, which was enforced by the NPCI. Though these applications are not subject to the governance of RBI, they undergo audits by the Banks and the NPCI.

This resulted in the creation of a hierarchy wherein the legislation was put on the top, circulars issues by the RBI and NPCI, followed by the standard operating procedures established by the institutions.

B. Evolution of the UPI Framework

The evolution follows a timeline from 2016. In 2016, the NPCI officially launched the Unified Payment Interface, allowing the participating banks to enjoy the feature of instant payments and transfer of money. In 2018, RBI released a data localization notification. Stating that all details with respect to digital payment systems must be stockpiled in India by the end of 6 months from the release of such a notification. This was followed by the announcement of NPCI in 2020 regarding the fixation of the market share at 30 percent. This was done in order to ensure that there is no dominant monopoly in the market. The implementation of this announcement has been prolonged, and the current deadline is December 2026. This postponement proved to be a huge relief to applications such as Google Pay. In 2021, RBI, through its e-mandates rules, removed the requirement of a one-time password (OTP) for transactions below 15000 Rupees. It, however, mandated the necessity of additional authentication in the form of an OTP for transactions exceeding the 15000 limits. The NPCI notification of 2022 allowed the linkage of credit cards under RuPay with the UPI platform. In 2023, the operational announcement of the UPI-Pay Now allowed international transactions within sixty seconds when done through banks liable under FEMA. Finally, in 2024, technical risks caused the Reserve Bank of India to announce a cap on the deposits made in the Paytm Payments Bank.

Every announcement, circular and notification made by RBI was after thorough examination of the impact of the Digital Payment Systems on the consumers and the intermediaries.

C. Primary Legislation Impacting Digital Wallets

1. Payment and Settlement Systems Act, 2007

This is the primary legislation responsible for overseeing the payments mechanism in India and this is inclusive of the Digital Payment Systems. The intention of enforcing this act is to maintain the reliability of the payment framework of India by warranting the Reserved Bank of India to supervise the operators of the digital payment systems. This act provided an introduction to the digital payment system by defining terms such as smart cards, digital transfers etc. This act mandates that all digital payment platforms must adhere to the guidelines issued by the Reserve Bank of India. It ensures that the e-wallets operate within the powers conferred upon them by the laws.

2. Reserve Bank of India Act, 1934

This act was responsible for hosting the Reserve Bank of India as the central bank in India. It conferred broad powers to RBI to ensure that all banking related organizations function as per the laws efficiently. Section 17 under this law permits RBI to operate in action as the central bank. This authority extends to the digital payment systems as well. It is responsible for granting the Bank with

the authority to regulate various transactions with respect to the banking sector and accommodates e-transactions within its purview.

3. Information Technology Act, 2000

This act's introduction created a landmark in terms of creating a revolution in the digital economy of India. By recognizing and legalizing electronic and digital signatures, it identified the need for electronic contracts and their importance in electronic payment transactions. Section 4 of the act establishes the legal validity of electronic records, making the existence of digital wallets legal. Further, through section 5, it defines digital signatures, allowing the signing of electronic transactions with respect to digital wallets.

4. Master Direction on Issuance and Operation of Prepaid Payment Instruments (PPIs).

In 2017, RBI issued a master direction under section 18 and section 10(2) of the Payment and Settlement Systems Act, 2007. It acts as a thorough guide for the operators of digital wallets regarding the interoperability and the regulation. It covered various aspects with respect to digital payments. In terms of eligibility, it stated that Banks are permitted to release limited use prepaid instruments and full use prepaid instruments post the approval of RBI. The prepaid instruments can achieve interoperability via the UPI framework by six months from the date from which the directions were released. For addressing the concerns regarding consumer protection, it mandated that all terms should be written in Hindi, English, and other necessary local languages. Further, an establishment of a grievance redressal framework was mandated that ensured that the complaints were addressed by minimum forty-eight hours and maximum by thirty days. Liability in case of fraud was highlighted to be zero when committed by the issuer and factors such as reporting time was considered while quantifying the liability.

D. Case Laws

The 2023 case of *Abhijit Mishra v. RBI & NPCI* was a landmark case with respect to platforms allowing digital payments in India. The petitioner in this case argued that since GooglePay was not authenticated by the Reserve Bank of India, it is unlawful to which the court held that the application was not replacing the Banks and was introduced in India as an external application provider after approval of NPCI and the overseeing banks.

Section 4 of the Payment and Settlement Systems Act, 2007 states that no individual other than Reserved Bank of India has the authority to initiate or run a payment system without explicit permission of the Reserved Bank.

In the 2025 case of *Supreme Court vs Securities Exchange Board of India*, a consumer had fallen

victim to a cyber fraud and the court ordered SBI to refund the entire subject matter amount of Rs 94,204.80 to the victim. The Defendant bank argued that the consumer had voluntarily shared the One Time Password, a means of authentication of transactions with a third party, making him ineligible for compensation and remedies. The court held that the notification circulated by RBI regarding the “zero liability in case of intimation within 3 days” would be invoked in this case. It was highlighted that the banks need to create a strong identification mechanism to prevent frauds such as these. The bank’s arguments were rejected, and the victim was granted the refund.

In 2024, the Rajesh Garg vs SBI was brought to the Chandigarh State Commission. In this case the victim (Rajesh) detected unsanctioned transactions from his bank account for the value of 64000 Rupees. The victim took immediate action in intimating the bank regarding the illegal transaction. However, SBI failed to revert the amount. The issue upheld in this case was whether the banks will be liable for fraudulent transactions when reported by the victim promptly. The court held that the bank was responsible for the deficiency in service due to its failure to respond to the victim’s grievance. This case highlighted the seriousness of the judiciary with respect to addressing the grievances of the consumers when they contract fraudulent activities in the digital payment systems.

E. International Perspectives: Global Regulatory Approaches to Digital Wallets

A. USA

The Digital payment transactions in this country are governed by the Electronic Fund Transfer Act. It provides a detailed framework for the governance of electronic payments, deposits etc. It offers the consumers strong protection against cyber frauds, unlawful transactions, and ensures that the operators provide all the necessary terms and disclosures for an individual to make an informed decision.

B. EU

The General Data Protection Regulation Act of EU is renowned in the world for its comprehensive coverage of digital payment systems and data protection laws. This act upkeeps the consumers to the highest level and ensures that cybercrimes and fraudulent digital transactions are penalized and the information with the operators are kept safe.

C. China

China implements the regulation of electronic payments through state-controlled platforms such as Alipay and We chat. All intermediaries in that country including financial institutions, ecommerce and other operate through these modes. Though regulations exist, the government directly exercises control over these platforms which exposes them to a risk of data breaches, and surveillance by the

Government.

IV. CONCLUSION

One of the most revolutionary financial developments in the global fintech scene is India's digital payment ecosystem, which is led by the quick uptake of the Unified Payments Interface (UPI). Although UPI has greatly improved financial inclusion, accessibility, and transaction efficiency, it has also made customers more vulnerable to changing legal and regulatory issues, especially in areas like cybersecurity, data protection, responsibility allocation, and dispute resolution.

This study shows that despite the Reserve Bank of India's (RBI) regulatory actions and the implementation of frameworks like the Digital Personal Data Protection Act, India has achieved impressive progress, but there are still gaps in providing strong consumer protection. Consumer confidence is still being undermined by problems like incomplete awareness systems, unclear accountability for unauthorised transactions, and delayed grievance redressal.
