International Journal of Global Research Innovations & Technology (IJGRIT)
An International Multidisciplinary Quarterly Double Blind Open Access Peer Reviewed Refereed Journal
ISSN : 2583-8717(Online), Impact Factor: (Cosmos: 6.972 & I2OR: 5.002), Volume 04, No. 04, October-December, 2026, pp 39-47

UPI and Digital Payment Fraud in India: Trends, Causes and Policy Responses

Dr. Vikram Meena[1] | Mr. Anil Kumar[2*]

[1,2]Assistant Professor, Shaheed Bhagat Singh College University of Delhi.

[*]Corresponding Author: anil.kumar@sbs.du.ac.in

Citation: Meena, V. & Kumar, A. (2026). UPI and Digital Payment Fraud in India: Trends, Causes and Policy Responses. International Journal of Global Research Innovations & Technology, 04(04), 39–47.

ABSTRACT

The last few years have seen dramatic changes to the payments landscape in India, and the introduction of the Unified Payments Interface (UPI) to the Indian payments ecosystem has ushered in a new era in India's payments experience with faster, easier, more inclusive and more cashless payments. Despite the benefits, the UPI ecosystem also suffers from problems of digital payments fraud, which can be offered with increased speed and convenience. This paper aims to analyze available secondary sources on the trends, reasons, and policies for Digital Payment and UPI fraud in India. The study is based on official sources and data published by the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), Government of India, and other related official sources. The focus of the study is to analyze the recent trends in UPI payments volume and value, the incremental risk of banking and digital payments fraud, the leading forms of fraud, the threats to the consumer and challenges posed by technology, and the government's and other institutions' changing regulations to mitigate the risks. This study focuses on phishing, vishing, manipulation of QR codes, fraudulent requests for payments, remote control scams, identity theft, and other social engineering scams. This study describes instant fraud monitoring, authentication, and speedy transaction intervention along with the importance of collaborations between institutions, consumer understanding, and technology risk assessment. This study recommends that the more ambitious project of the digital-payment ecosystem's sustained growth in India anticipates a balanced integration of policy, innovation, convenience, security, and accountability, and most importantly, the interests of consumers.

***Keywords**: UPI, Digital Payments, Payment Fraud, Cyber Fraud, Financial Fraud, Digital Banking, Consumer Protection, Cybersecurity, NPCI, RBI, India.*

Introduction

Digital technology has rapidly changed the financial system and workplace structures in India. The last decade has seen unprecedented progress in digital payments, transforming cash payments from a "not to outs-and-back" option to a significant contributor to economic activities. (Bhatt, 2025) The Unified Payments Interface (UPI) is a phone-based innovation that facilitates instant bank-to-bank transfers. Because of UPI's interoperability, convenience, high merchant acceptance, and low transaction friction, it has been widely adopted by businesses, banks, and customers (Bhatt, 2025). With the advent of UPI, electronic commerce, small value retail transactions, peer-to-peer transactions, and the financial integration of consumers has greatly expanded. (Kiran, 2025). However, new opportunities by UPI also means that India now faces threats posed by financial actors, especially risks posed by cyber payment fraud. Some of the methods used by fraudsters exploit people (primarily lack of digital literacy and online security) and/or the gaps and weaknesses present in digital technology. (Fraud chasing, exploiting weaknesses and gaps in the digital realm, 2025). The design of UPI makes it difficult to stop fraudulent

Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.

payments. Banks, payment-service providers, policymakers, and customers all consider security as a critical part of the execution of digital payments (Lonkar, A., 2024). This paper examines how digital-payment scams and the swifter growth of UPI in India are connected. This paper analyzes official statistics in India pertaining to the growth of UPI and the reported cases of banking and/or electronic payment fraud. This paper attempts to identify the primary causes and means of fraud and assesses the institutional and regulatory actions undertaken for the frauds (Ligon, E., 2019). This paper contributes to the area of Commerce, as securely offering digital-payment infrastructure is a building block of an inclusive and growing economy and a trusting citizenry, as well as a healthy and growing digital economy in India (Mandal, T., 2024).

Background and Rationale of the Study

As the Digital economy grows so do financial cyber crimes. It is important to analyze UPI and digital payment fraud in the current context. Rapid expansion of UPI services and Official NPCI statistics show increasing volume and value. According to RBI reports, card/internet fraud is a dominant banking fraud (Mukhopadhyay, N., 2024). Although correlating UPI fraud numbers to broader card/internet fraud is difficult, it gives us an understanding of the maturity and extent of the digital channel of fraud in the Indian context. The central question is not whether UPI is a financial fraud facilitator in itself, but what financial fraud opportunities, vulnerabilities, and institutional needs may be affected by the expanding digital payments infrastructure (Pahari, S., 2023)? It is important to consider the distinction between technological fraud and consumer-related fraud because many of the fraudulent transactions investigated by the study involve social engineering and the approval of the end user. Knowing how preventive policies work is vital to understanding what drives their effectiveness (Pal, A., 2021). With this in mind, this paper analyzes the prevalence of fraud and significant fraud techniques and the consumer and regulatory (from the Reserve Bank of India (RBI) and National Payments Corporation of India (NPCI)) focus. The aim is to provide a data-based analysis of the significant problems facing the digital payment system in India. It examines the trends in the growth of digital transactions, and fraud and policy data (Rastogi, S., 2021). The results will aid the discussions on a number of contemporary problems such as cyber security, customer protection, financial literacy and the sustainability of banking and digital commerce in India.

Literature Reviews

Raghavendra, V. (2023) also addressed the rise of banking fraud in India and how digital banking and card/internet banking have become increasingly important. As more methods become more electronic, fraud related to the internet are beginning to be reported more, the report says. Consumers and businesses are starting to rely on these methods of electronic payments more. Emerging risks are vulnerabilities of technology and customer awareness; social engineering, and phishing attacks, the report says. It also stresses the importance of the oversight and management of fraud risk and how it will need to be more intense, as digital transactions happen more rapidly. The RBI states the importance of early-warning detection systems along with more efforts in governance, customer awareness, and strengthening online banking, while also stating the importance of red flag detection systems. The importance of the report for this study is that it shows the growth of digital payment systems in India and the risk of fraud that is associated with this increase. The report states the importance of understanding the difference between digital payment fraud and the rest of the banking fraud to help determine the risks associated with the UPI.

Sharma, A. (2024) UPI, United Payments Interface, is banking infrastructure designed for India's retail payments. UPI has grown exponentially and is Transaction Processing Billions (TPBS). UPI's growth in volume and value has been attributed to the growing adoption of UPI by consumers, merchants, and banks/payment service providers. The rapid growth of UPI has enhanced person-to-person (P2P) payments and person-to-merchant (P2M) payments. The Indian government is actively moving towards creating a cashless economy. However, rapid growth comes with some disadvantages. UPI has become a platform for transactions involving real-time payments. This means that the possibility for transactions fraud is very real and will be easily exploitable. The focus on security frameworks, authentication, ecosystem controls, and transaction safeguards means that growth in technology is directly proportional to the growth in security. The PCIs focus on security frameworks, authentication, ecosystem control and transaction safeguards further illustrates that growth in technology and security happens in parallel. This is applicable to this study, as it presents the first and principal base upon which the literature on the development and the increasing importance of UPI in the digital commerce landscape in India is built.

Sharma, A. (2024) Progress in digital payments and technology is expanding India's increasingly complex Consumer Protection and Cyber Security. The Report states that electronic banking and payment systems improved the speed and ease of banking, but created operational and cyber risks. They focused on the needs of consumers to be aware and in control of transactions through safe and secure authentication and the reporting of fraud and assurance of redress. Digital fraud does not require sophisticated hacking of payment systems. It relies on fraudulent methods. Financial security subsequently relies on understanding consumer payment behavior. The Reserve Bank of India's approach consists of two types of controls; one, institutional control, and, two, consumer control, which includes the initiation of more programs for consumer awareness and frameworks for resolution of consumer complaints against unauthorized payments. The literature supports the Banking and Payment System control as being more about participatory cooperation than technology. The most relevant case is UPI. UPI facilitates instant payments, which results in customers being unable to withdraw payments following authorization.

Singh, S. K. (2023) documented the impacts of cyber-financial crimes and the counter measures that have been developed. The government's mostly fast-response strategy to suspected fraud comprises four elements, namely focus on integrity in the cybercrime reporting process, enhanced coordination among law-enforcement, banking, and financial sectors, and better coordination of suspected fraud cases. The establishment and the gradual improvement of specialized reporting and coordination institutions for cybercrime demonstrate that digital financial crime cannot be addressed in the traditional way of banking and requires special investigating and technological tools. Further, it has been recognized that most digital payment frauds are done through spoofing of URLs, impersonation, misrepresentation, fake sales customer support, and social engineering. Hence, integrated policy responses which incorporate behavioral, technological, and institutional tools are required. This would be an important starting point for the analysis of policy response to UPI related frauds as this clearly shows that many stakeholders from banking, technology, and law enforcement must be involved in the effort to curb fraud.

Methodology

- **Research Design and Approach**

This study uses case-based, descriptive, and analytical techniques to examine the expansion of the United Nations Inter-case Check (UNIC) Unified Payments Interface (UPI) in India. It also evaluates trends in digital payment fraud, focuses on the reasons, reviews the government's responses, and analyzes the policies and laws. Due to the national scope, this study uses secondary and quantitative data, and draws upon documentation. As longitudinal studies of UPI transactions enable the tracking of volumes and the values of the transactions and of banking and digital payment and fraud cases, the author uses this data to fill this research gap. This study aims to distinguish the statistics of UPI transactions from those of digital payment and credit card and internet fraud; the official fraud files do not distinguish UPI fraud transactions. Digital, or credit card and internet fraud, is not treated as UPI fraud in the analysis. Descriptive techniques such as percentage changes, growth rates, and comparisons are employed to analyze the evidence. This research uses a qualitative policy analysis framework to determine regulations against Indian authorities and financial institutions and to investigate the institutional infrastructure, cyber security, and consumer protection, as well as the strategies to combat fraud.

- **Sources of Data**

This study uses genuine secondhand data from authorised Institutions in India. NPCI has been collecting UPI transactions in volume and value for monthly and annual records. The Annual Reports of the Reserve Bank of India (RBI) and their statistical publications have banking fraud data, including details of banking fraud cases, banking fraud amounts, banking fraud types, and the trend of banking fraud, including card frauds and online fraud. Further information on the protection of consumers and the security of digital payments and Internet crime is available from various official sources of the Government of India, the Ministry of Finance, the Ministry of Electronics and Information Technology, the Indian Cyber Crime Coordination Center (I4C), and other official publications. For the time period 2018-19 to 2025-26 is the primary analysis time frame, provided officials SDS are available/ similar. For providing theoretical and contextual support, reviews of research papers and policy documents and other reports are used. Information from secondary sources is not considered primary data if official information is available.

- **Variables, Indicators and Data Period**

This study employs quantitative and qualitative methods. It does this using indicators for UPI and digital payment fraud monitoring in India. The main UPI metrics are annual transaction value and volume, monthly transactions, and growth in the number of transactions for the year under consideration. Fraud indicators are reported cases of fraud, the value of fraud, the type of fraud, the region that fraudulent activities were reported, and the card/online fraud trends. Where appropriate data are available, the study researches the ratio of transaction growth and fraud exposure. The qualitative indicators refer to the dominant fraud techniques, consumer weaknesses, technology gaps, institutional and regulatory responses, and cyber security. The fast growth rate of the digital/electronic payment systems in India sets the time frame for the proposed research 2018-19 and 2025-26. The numbers of frauds may vary from year to year and by various categories. Thus each data set will be analyzed for the time of reporting, the way it is described and the way it is classified, and no assumptions will be made. This approach promises to give more reliable results that can be compared.

- **Data Analysis Techniques**

To analyze information, descriptions and analyses are used to sort, arrange and tabulate data to answer questions. A trend analysis of annual values and volumes of UPI transactions is used to show the direction and the extent of digital payments. Data are consistent enough to enable calculation of year-on-year and compound annual growth rates. The fraud data are used to analyze changes in the sizes and types of fraud that occur. Measure the amount involved, the fraud category and the region to determine the type of fraud. To understand the fraud trends, compare the financial years that have been selected. Investigations make use of tables, charts and graphs to summarize the information. The objectives of the paper are to present the UPI data on the growth of transactions and compare them to the data on the growth of card internet and banking fraud. A policy paper is drafted after reviewing NPCI and RBI circulars, government measures, and institutions dealing with cybercrimes. The methodologies of policy and documentation are applied. The study considers consumer behavior, the limitations of technology and institutional capacity as well as regulatory performance. While the integrated methodology enables the study to give an evidence-based analysis of digital-payment fraud in India, it also ensures local relevance. This is achieved by integrating different stakeholders, jurisdictions and national organizations.

Results and Analysis

- **Growth and Trends of UPI Transactions in India**

The results show UPI's large role in India's growing digital payments system. Data from the last several years show an increase in transaction volume and an even greater increase in value. Transactions in UPI increased by 250 times from ₹84.16 lakh crore in FY 2021–22 to a peak of ₹314.23 lakh crore in FY 2025–26, and the number of transactions also increased by two times from 4,595.61 crore to 24,161.69 crore in FY 2025–26. Because of these numbers in the last several years, UPI has established itself as a fundamental part of IndianRetail's digital payment system. The reason there has been such a large increase in transactions has been the constant growth of consumer spending, more merchants creating the means for transactions, more smart devices, and the ability of different payment systems to communicate with each other. Additionally, there is clear evidence UPI's dominance in digital transactions is getting stronger shown by the continued strong growth even after the large initial numbers of transactions.

Table 1: Growth of UPI Transactions in India

Financial Year	Volume (Crore Transactions)	Value (₹ lakh Crore)
2021–22	4,595.61	84.16
2022–23	8,371.44	139.15
2023–24	13,112.95	199.95
2024–25	18,586.60	260.56
2025–26	24,161.69	314.23

Source: National Payments Corporation of India (NPCI) UPI statistics; Government of India, Ministry of Finance/PIB, 2026.

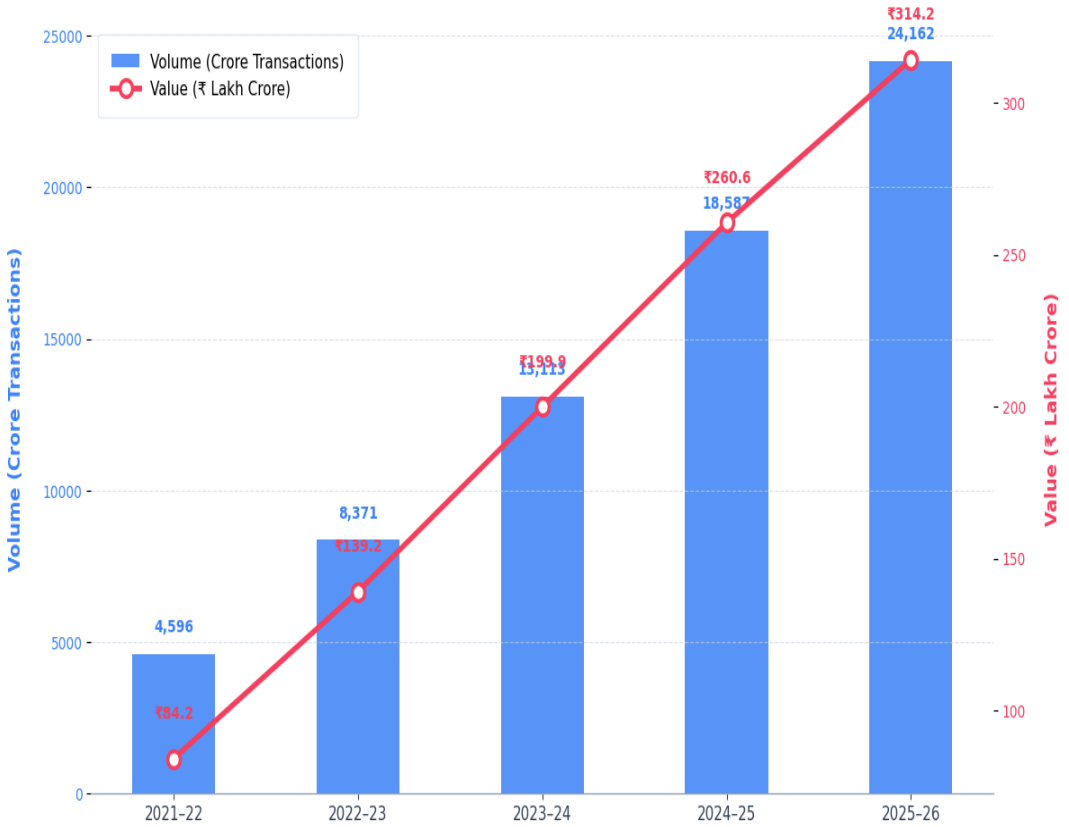

Figure 1: Growth of UPI Transactions in India (2021–2026)

- **Trends and Patterns of Digital Payment and Banking Fraud**

The second important finding concerns the changing patterns of banking fraud reporting. As per RBI, card/internet fraud has started to pile up in terms of cases, whereas the highest monetary amounts have been observed in the advances or loan portfolio. In the financial year 2023–24, 29,082 cases worth 1457 crore (≈$1 billion USD) were reported. Card/Internet fraud has consistently been the highest case number fraud in a financial year with 13,516 cases and 520 crore rupees lost. However, overall banking fraud cannot be equated to UPI fraud because bank/Internet card fraud is segregated into different channels. This distinction is important for a sound interpretation of the results.

Table 2: Reported Bank Frauds by Area of Operation

Area of Operation	2022–23 Cases	Amount (₹ crore)	2023–24 Cases	Amount (₹ crore)	2024–25 Cases	Amount (₹ crore)
Advances	4,021	17,542	4,118	10,072	7,950	33,148
Card/Internet	6,699	278	29,082	1,457	13,516	520
Deposits	652	259	2,002	240	1,208	527
Cash	1,485	159	484	78	306	39
Others	637	743	374	383	973	1,780
Total	13,494	18,981	36,060	12,230	23,953	36,014

Source: Reserve Bank of India, Annual Report 2024–25, Table VI.3, RBI Supervisory Returns.

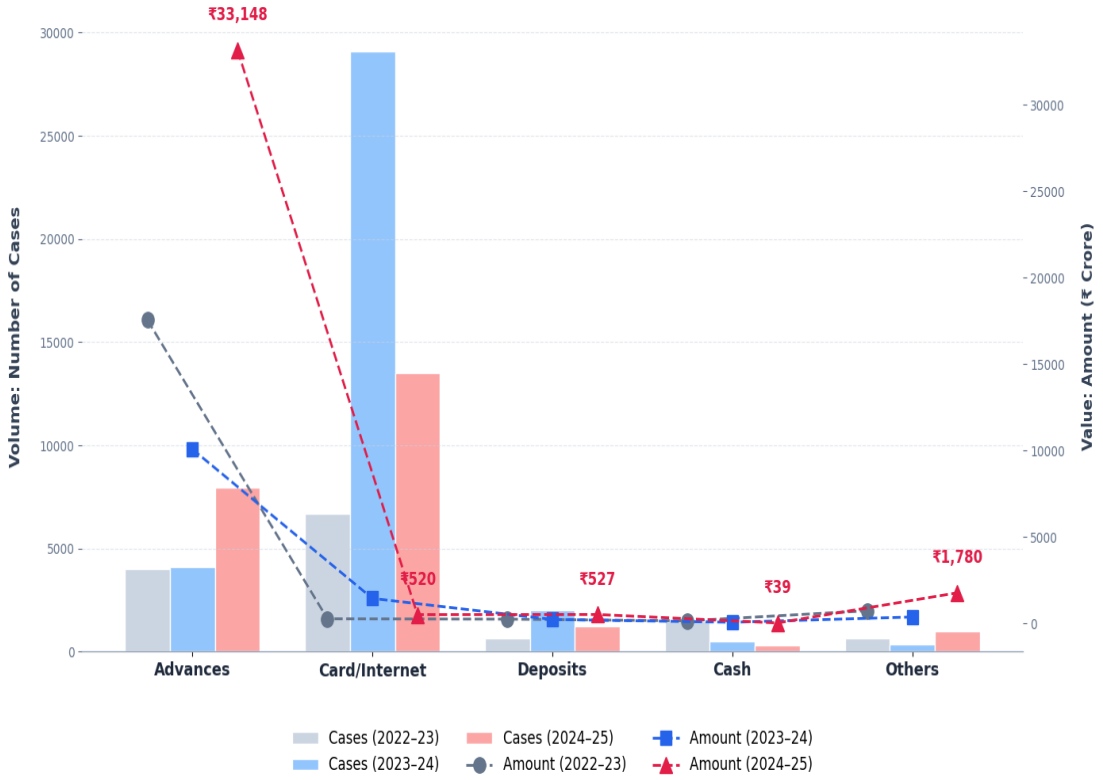

Figure 2: Bank Frauds Volume vs. Value (2022–2025)

- **Major Causes and Mechanisms of Digital Payment Fraud**

The analysis reported that the main causes of digital payment fraud in India are a combination of technological, behavioral, and organizational issues. Because most UPI transactions are completed at speeds that are nearly real-time, once a payment is authorized, there is very little time intervene in cases of fraudulent transactions. Though fraudsters do not target UPI infrastructure, they do target UPI users. Common techniques used by fraudsters include impersonating customer service, providing fake QR codes, getting people to divulge payment details by clicking on web links or through apps used in remote payment systems, and making deceptive calls. RBI's payment systems payment fraud indicators show that payment fraud remains pervasive across the payment systems in India. The recorded value of domestic payment fraud increased from ₹249 crore in September 2022 to ₹507 crore in February 2024, which is an indication that domestic payment systems, and not just UPI, are experiencing an increase in reported payment fraud. The value of domestic payment fraud for UPI should not be used for this comparison.

Table 3: Selected Domestic Payment Fraud Indicators

Month	Fraud Volume (lakh)	Fraud Value (₹ crore)	Fraud-to-Payment Value (bps)
September 2022	1.71	249	0.127
December 2022	1.54	204	0.103
March 2023	2.25	333	0.142
September 2023	2.52	366	0.174
December 2023	2.92	432	0.187
January 2024	2.69	435	0.207
February 2024	2.53	503	0.239
March 2024	2.57	471	0.177

Source: Reserve Bank of India, Payment System Indicators, Part V—Domestic Payment Frauds. Data are provisional and cover domestic payment transactions across the payment system.

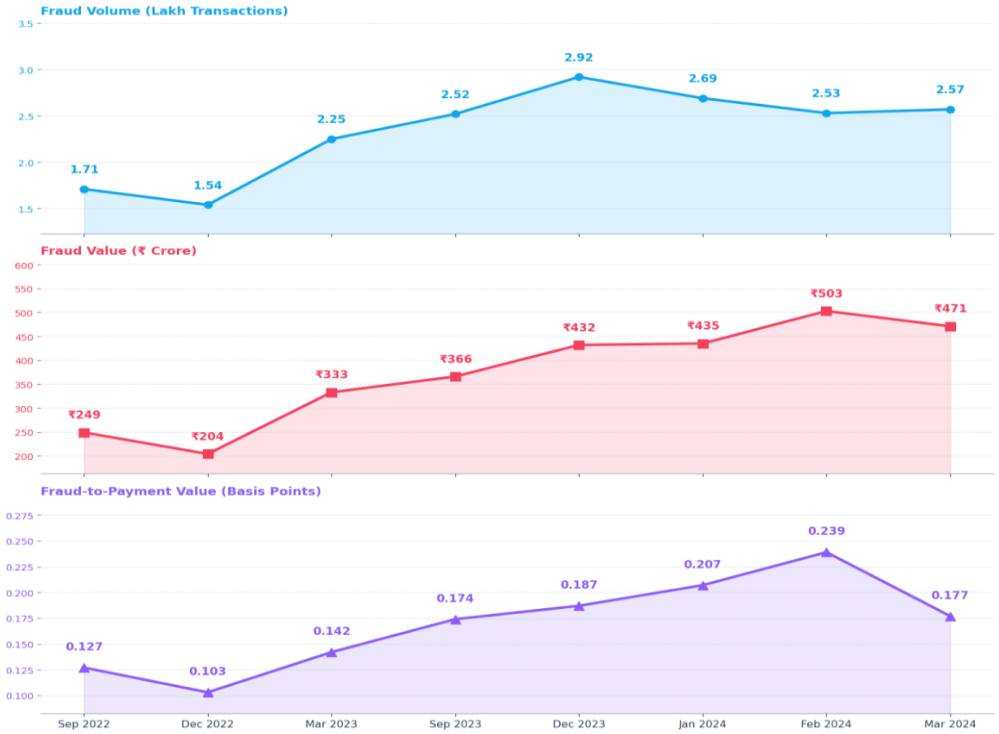

Figure 3: Selected Domestic Payment Fraud Indicators (Sep 2022 – Mar 2024)

- **Policy and Institutional Responses to Digital Payment Fraud**

India has established an integrated system for preventing, monitoring, and controlling digital payment fraud using the P2P payment system. The RBI (Reserve Bank of India) has introduced more effective techniques for managing fraud and cyber risks and has implemented full C-V (Consumer Protection) Framework. Meanwhile, the NPCI (National Payments Corporation of India) has continued to develop the UPI ecosystem and introduced new security measures. In 2024-25, RBI made changes to their Master Directions focused on fraud risk management and enhanced the Early Warning Signals and the Red flag Recommendations. RBI reported that more advanced methods of analytics, such as AI (Artificial Intelligence) and ML (Machine Learning) modeling, have been used to perform fraud risk assessments and as a basis for supervisory analysis. A series of measures was announced by the Government to make UPI (Unified Payment Interface) transactions safer in 2026. As a result, all UPI transactions were limited to a specific app. The Compliance UPI Information Security Framework (CUISF) 2025, the Mobile App Security Framework, and other security frameworks were also published.

Table 4: Major Policy and Institutional Responses

Institution/Measure	Major Intervention	Primary Objective
RBI	Revised Fraud Risk Management Directions, 2024	Strengthen fraud governance and early detection
RBI	Early Warning Signals/Red Flagging	Identify suspicious activities
RBI	AI/ML-based supervisory analytics	Improve fraud-risk identification
RBI	Cybersecurity and digital-channel resilience measures	Strengthen digital banking security
NPCI	UPI security frameworks	Improve UPI ecosystem resilience
Government/RBI/NPCI	Risk-based transaction limits	Reduce potential fraudulent exposure
RBI	Consumer awareness and grievance mechanisms	Improve protection and redressal
RBI Ombudsman system	Complaint and grievance resolution	Support affected customers

Source: Reserve Bank of India Annual Report 2024–25; Government of India, Ministry of Finance/PIB, July 2026; NPCI official UPI information.

Discussion

UPI's fast adoption by users and financial institutions has significantly altered India's digital payment landscape and added risks of digital payment fraud to consumers and financial institutions. The large and rapid growth in the value and volume of UPI transactions and the resulting high velocity of UPI transactions increases the opportunities for scammers. Most of the reported frauds fall into the category of Digital and Card/Internet fraud. However, in its classification, the RBI includes several digital payment systems. Distinguishing strategies to understand the development of UPI and fraud are valuable. In most cases, social engineering, phishing, impersonation, and fraudulent payment requests occur more frequently than technical flaws. The resulting policy interventions have reduced the prevalence of frauds and risks. Cybersecurity and customer awareness have also been significantly improved, as have the scope and quality of collaboration between institutions. The best way to ensure the success of these initiatives is to ensure that suspicious transactions are identified and actions are taken before funds are transferred. India's future digital payment systems should consider a combination of behavioral control systems and real-time grievances, technology-based systems, and digital literacy. This balance enables real-time digital payments while preserving the customer's trust and installing protections.

Conclusion

This study describes how the Unified Payments Interface (UPI) has shaped transactions between individuals, businesses, merchants, and financial institutions as a part of the digital economy of India. Data from the government of India shows how UPI transactions have grown in both volume and value, demonstrating how UPI is winning the confidence of customers, how merchants are adopting UPI, the ease of using UPI, and how digital payments have been integrated into the business activities of merchants. However, the increase in digital transactions has also posed an increased risk of financial fraud. This is trues with the increased risk of cyber crimes. Statistics show that many of the banking frauds reported are cases of frauds committed using cards or through the internet, which uses many electronic channels and are not limited to UPI. The report states that customers of digital payment transactions are vulnerable to phishing, vishing, social engineering, fake customer care sites, false payment requests, a lack of customer sophistication, apps to access the internet and fraudulent QR codes. There has been promising work done by RBI regulations, NFCI's security measures, fraud-risk management systems and awareness programs. However, the work done by fraud-risk management systems will only be effective if banks, payment service providers, regulators and law enforcement do: act fast, they intervene, and they coordinate. Given the above research, we recommend these strategies to combat real-time fraud: real-time fraud analytics, quick suspension of potentially fraudulent transactions, consumer education, and information exchange within the payment ecosystem. As UPI evolves, it is essential to preserve the speed and convenience of the service. This will help maintain an inclusive service that protects the interests of all users and meets the needs of the marketplace while guarding against fraud and protecting consumers.

References

1. Bhatt, I. (2025). Red flags in UPI (Unified Payments Interface): A study on digital payments in India. *NFSU Journal of Forensic Accounting & Fraud Investigation*.
2. Gupta, R., Anand, A., & Gupta, T. (2025). Are digital payments driven by wealth inequality? Evidence from analysis of the Unified Payments Interface (UPI) adoption in India. *Economic Analysis and Policy, 87*, 1130–1141.
3. Kiran, K. P., & Sailaja, V. N. (2025). Assessing Unified Payments Interface (UPI) adoption and usage through the interplay of UTAUT factors. *Humanities and Social Sciences Communications, 12*, Article 1060.
4. Kiran, K. P., & Sailaja, V. N. (2025). Exploring behavioral intentions of consumers towards different digital payment services through the interplay of perceived risks and adoption factors. *Humanities and Social Sciences Communications, 12*, Article 1141.
5. Lonkar, A., Dharmadhikari, S., Dharurkar, N., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: A study of consumer preparedness in India. *Journal of Financial Crime, 32*(2), 257–278.
6. Ligon, E., Malick, B., Sheth, K., & Trachtman, C. (2019). What explains low adoption of digital payment technologies? Evidence from small-scale merchants in Jaipur, India. *PLOS ONE, 14*(7), e0219450.

7. Mandal, T. (2024). Adoption of UPI and implementation of UPI-ATM in India: A logit analysis. *Indian Journal of Economics and Finance*.

8. Mukhopadhyay, N., & Mukhopadhyay, M. (2024). UPI frauds: A study on UPI usage, awareness and impact in India. *International Journal of Research in Commerce and Management Studies, 6*(6), 179–197.

9. Pahari, S., Manna, A., & Biswas, D. (2023). Pay with confidence: A thematic analysis of user intentions and perceptions on third-party and banking payment apps. *Indian Journal of Finance, 17*(5), 25–38.

10. Pal, A., Herath, T., De', R., & Raghav Rao, H. (2021). Why do people use mobile payment technologies and why would they continue? An examination and implications from India. *Research Policy, 50*(6), 104228.

11. Rastogi, S., Panse, C., Sharma, A., & Bhimavarapu, V. M. (2021). Unified Payment Interface (UPI): A digital innovation and its impact on financial inclusion and economic development. *Universal Journal of Accounting and Finance, 9*(3), 518–530.

12. Raghavendra, V., & Veeresha, P. (2023). Analysing the market for digital payments in India using the predator-prey model. *An International Journal of Optimization and Control: Theories & Applications, 13*(1), 104–115.

13. Saxena, S., & Yadav, A. (2025). Domestic payment frauds in India (2022–2025): A quantitative analysis of trends, risk indicators, and policy implications. *NOLEGEIN Journal of Business Risk Management*.

14. Sharma, A., & Singh, Y. (2024). Cyber frauds in India's digital payment ecosystem: Risk, impacts, and regulatory responses. *Educational Administration: Theory and Practice, 30*(5), 15326–15332.

15. Singh, S. K., Singh, S. S., & Singh, V. L. (2023). Predicting adoption of next generation digital technology utilizing the adoption-diffusion model fit: The case of mobile payments interface in an emerging economy. *ACCESS: Journal of Science, Business, Innovation in the Digital Economy*.

