Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

UPI Fraud and Consumer Protection: Examining Bank Liability for Digital Payment Fraud

S Sai Pranitha[a] Gorriparti Naresh[b]

[a]KL University, Guntur, India [a]Assistant Professor, KL University, Guntur, India

Received 14 September 2026; *Accepted* 14 October 2026; *Published* 19 October 2026

The widespread adoption of the Unified Payments Interface (UPI) has led to a complete transformation of the retail payment ecosystem in India towards achieving financial inclusion and developing a cashless economy. However, this revolution is also characterised by the advancement of digital payment fraud, moving from the compromise of technical systems to intricate social engineering schemes and 'Authorised' Push-Payment (APP) fraud. This research paper attempts to understand the issue of UPI fraud and consumer protection with special attention to the evolving legal environment concerning bank liability in India. Applying qualitative content analysis of the Reserve Bank of India (RBI) circulars, the Payment and Settlement Systems Act 2007, the Information Technology Act 2000, and the Consumer Protection Act 2019, this study evaluates the effectiveness of existing mechanisms for protecting consumers from bank fraud. It was found that while the RBI created a hierarchical responsibility scheme for unauthorised transactions, there is a huge regulatory gap in relation to fraud cases where consumers themselves authorise payments due to manipulation. In order to investigate this problem in-depth, this study analyses technological advancements. In addition, it takes into account comparative lessons learned from other countries like the United Kingdom, the European Union, Nigeria, and Colombia for a more balanced loss-sharing scheme. The paper concludes that solving the 'liability gap' in social engineering fraud cases needs a combination of solutions, which include the following: real-time fraud detection, increased digital literacy, and changes to laws on the responsibility of banks and non-bank third-party payment applications.

Keywords: *UPI fraud, bank liability, consumer protection, social engineering, digital payments.*

INTRODUCTION

There has been an unprecedented boom in the Indian digital payments landscape, driven primarily by the implementation of the UPI (Unified Payments Interface) in 2016.[1] The open-architecture platform provided by NPCI enables inter-bank payments in real time and has served as an important part of the 'Digital India' program.[2] The success of this platform has been confirmed by its use across various demographics, such as Gen X[3] and grocery store retailers,[4] who have shifted to cashless payments for their efficiency and speed. In India, the volume of digital transactions has grown by a factor of 38 times by 2025, which is evidence of a change in consumer behaviour due to macro-economic shocks such as the demonetization of 2016 and the coronavirus pandemic.[5]

Nevertheless, this speedy adaptation has unveiled certain system weaknesses that are increasingly used by cyber criminals.[6] Frauds related to online banking in India have progressed beyond the traditional phishing scams to include an array of cybercrimes such as identity frauds, adaptive malware, and deepfake technology-based frauds. Such frauds are very dangerous and not only threaten the personal safety of individuals' finances, but they also have a detrimental effect on the entire digital economy. In the case of UPI fraud, there

[1] A Mahesh and G Bhat, 'Digital Payment Service in India – A Case Study of Unified Payment Interface' (2021) 5(1) International Journal of Case Studies in Business, IT and Education <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3885763> accessed 10 September 2026

[2] Rahul Kumar Agarwal and Dr Diganta Kumar Das, 'UNIFIED PAYMENTS INTERFACE (UPI) REVOLUTION: TRANSFORMING DIGITAL PAYMENTS IN INDIA' (2023) 3 <https://doi.org/10.58532/v3bhma2p3ch4> accessed 10 September 2026

[3] Vaishali Solanki and Dr Gaurav Rajput, 'Sustainable Digital Payments: Examining Unified Payment Interfaces (UPI) Adoption Among Generation X' (2025) 4(24) International Journal of Environmental Sciences <https://theaspd.com/index.php/ijes/article/view/10343/7416> accessed 10 September 2026

[4] Miss Shweta D Gupta, 'Impact of E-Payment on Retail Grocery Shops (With Reference to Nagpur City)' (2022) 2(2) International Journal of Advanced Research in Science, Communication and Technology <https://ijarsct.co.in/A7430.pdf> accessed 10 September 2026

[5] Mahesh A & Ganesh Bhat S, 'India's Digital Payment Landscape – An Analysis' (2022) 6(1) International Journal of Case Studies in Business, IT, and Education <https://www.researchgate.net/deref/https%3A%2F%2Fdoi.org%2F10.5281%2Fzenodo.6467728?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19> accessed 10 September 2026

[6] Prof Ritika Maini and Prof Vivek Kumar Sindhi, 'Digital Banking Fraud in India: Typologies, Victim Behaviour, and AI-Enabled Risk Governance in a Global Context' (2025) 7(5) International Journal for Multidisciplinary Research <https://doi.org/10.36948/ijfmr.2025.v07i05.55593> accessed 10 September 2026

has been a shift towards 'Authorised Push Payment (APP)' fraud, which is basically the manipulation of victims into paying through psychological pressure.[7]

However, the existing regulatory environment, with its focus on RBI liability circulars and the Consumer Protection Act of 2019, finds it difficult to cope with such 'legal' frauds.[8] Though the intention behind regulation is to protect the customer against any failure at the system level, the responsibility for security lies increasingly on the shoulders of the smartphone and the individual himself. In this paper, the current state of bank liability, technical solutions such as AI-based detection systems, and the existing loopholes in Indian law will be discussed.

LITERATURE REVIEW

Digital payment fraud literature is divided into two groups: works that concentrate on technical aspects of the issue and those that look at socio-legal aspects of risk management.[9] Singh (2025) points out that although open API integration has made it possible for smooth inter-bank transactions, it has at the same time created possibilities for fraud, such as credential fraud and data access fraud.[10] UPI frauds are discussed extensively in the article by Maini et al. (2025), where the authors identify QR code frauds and misuse of request money as the main categories of UPI fraud, with the behaviour of victims being affected due to their lack of digital literacy and shame.

However, technological advancements have been at the forefront of the fight against fraud. According to the study by Kumari et al. (2025), there have been attempts to use complex AI techniques such as Random Forest, Naïve Bayes, and SVM to fight deepfake fraud.[11] Using behavioural biometrics and network analysis, transaction patterns can be monitored in real

[7] Jo Braithwaite, ''Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?' (2024) 10(2) Journal of Financial Regulation https://doi.org/10.1093/jfr/fjae006> accessed 10 September 2026

[8] Adhip Banerjee et al., 'Digital Payments in India: Exploring Emerging Issues in the Legal and Regulatory Framework' (2025) 17(1) Krytyka Prawa <https://doi.org/10.7206/kp.2080-1084.753> accessed 10 September 2026

[9] Amit Kumar Singh and Prof Krishna Kumar Agarwal, 'AN OVERVIEW OF DIGITAL PAYMENT FRAUDS: CAUSES, CONSEQUENCES, AND COUNTERMEASURES' (2025) 5(1) Journal of Informatics Education and Research <https://doi.org/10.52783/jier.v5i1.2230> accessed 10 September 2026

[10] Reema Singh, 'Fraud Risks in Open API Implementation: A Comparative Study of India and International Financial Markets' (2025) Economic Consultant <https://doi.org/10.46224/ecoc.2025.1.4> accessed 10 September 2026

[11] Dr D Jaya Kumari et al., 'AI-Powered UPI Fraud Detection' (2025) 10(4) International Journal of Innovative Science and Research Technology <https://doi.org/10.38124/ijisrt/25apr830> accessed 10 September 2026

time to identify unusual behaviours.[12] Moreover, the RBI's MuleHunter.AI project is aimed at the identification of mules whose services are critical for laundering the proceeds from online scams.[13] In addition, machine learning approaches have also been considered for improving detection within the environment without sacrificing sensitive user information.[14]

Nevertheless, the success of such controls is often marred by the human factor. Social engineering, which involves using psychological tricks on people to circumvent technical security measures, is still the greatest challenge.[15] Braithwaite (2024)[16] and Maher (2024)[17] evaluate how the UK has handled regulation in response to APP fraud, given that the normal agreements between banks and their customers make the customers responsible for the loss due to the 'authorisation' of the transaction. This has brought about discussions in the international community regarding the 'Predictably Irrational Customers' concept.[18]

The legal aspect in India is based on the Information Technology (IT) Act, 2000,[19] and the Payment and Settlement Systems (PSS) Act, 2007.[20] According to Chakraborty and Rana (2025), the Indian Information Technology Act is similar to US laws on cyberspace, but India needs specific laws defining fraud and better enforcement to safeguard online banking clients.[21] With the increase in fintech banking services, there are now some new threats of data breaches and account linking, which require a revision in the existing data protection

---

[12] Ms Krisha Rakesh Patel, 'Cybersecurity in Digital India: Enhancing UPI Security with AI-Driven Behavioral Biometrics' (2025) Zenodo <https://doi.org/10.5281/zenodo.17228089> accessed 10 September 2026

[13] *Statement on Developmental and Regulatory Policies* (Reserve Bank of India, 2024)

[14] Deepa Devassy et al., 'FedUPI: Federated Learning Empowered Detection of Fraudulent UPI Transactions' (Conference: 5th International Conference on Soft Computing for Security Applications (ICSCSA), Salem, India, 2025)

[15] Putu Devi Yustisia Utami and Ni Putu Purwanti, 'STRENGTHENING LEGAL PROTECTIONS AGAINST SOCIAL ENGINEERING IN DIGITAL BANKING: CHALLENGES, GAPS, AND RECOMMENDATIONS' (2025) 54(2) Masalah-Masalah Hukum <https://doi.org/10.14710/mmh.54.2.2025.214-226> accessed 10 September 2026

[16] Braithwaite (n 7)

[17] Robyn Maher, 'A CRITICAL ANALYSIS OF RECENT EFFORTS IN THE UNITED KINGDOM TO TACKLE AUTHORISED PUSH PAYMENT SCAMS AND THE IMPACT ON THE BANK-CUSTOMER RELATIONSHIP' (2021) 24 Trinity College Law Review <https://access.heinonline.com/HOL/LandingPage?handle=hein.journals/trinclr24&div=12&id=&page=> accessed 10 September 2026

[18] Junqi Wang and Duwei Deng, 'Unauthorized Transactions and Unintended Transactions in Open Banking: Loss Allocation Based on Predictably Irrational Customers' (Conference: 6th Annual International Conference on Social Science and Contemporary Humanity Development (SSCHD), Xi'an, Shaanxi, China, 2020)

[19] Information Technology Act 2000

[20] Payment and Settlement Systems Act 2007

[21] Jayasmith Chakraborty and Abhishek Singh Rana, 'CYBER FRAUD IN DIGITAL BANKING AND UPI: A COMPARATIVE ANALYSIS OF THE INDIAN IT ACT, 2000 AND U.S CYBER LAW FRAMEWORK' (2026) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6647799> accessed 10 September 2026

framework. Research conducted in various states of India shows considerable differences in the 'Cyber Payments Maturity' of the states.

RESEARCH GAP

Although there have been many studies on the economic effect of UPI[22], in addition to general cybersecurity threats, there is a clear gap in the literature in terms of the 'liability vacuum' for social engineering fraud in India. The majority of the available literature is either concerned with the technical aspects of fraud detection or legal issues related to the unauthorised use of systems (system hacking). There is very little scholarly discussion in relation to the bank's liability in the case of authorised fraud where the second factor of authentication (AFA) is obtained through coercion/deception.[23] Moreover, the liability chain involving third-party payment application providers (TPAPs) is not adequately addressed in India's statute laws, thus giving rise to uncertainties whenever more than one party is involved in a dispute (e.g. banks, payment gateways, application developers).[24] The difficulty of obtaining evidence for such cases in consumer tribunals is another area of concern for future research.[25]

STATEMENT OF PROBLEM

The core issue in the UPI network is the discrepancy between the speed at which transactions take place and the speed at which remediation can occur legally and technologically. UPI supports instant, irreversible transactions, which makes it possible for scammers to empty out the account and transfer funds through multiple mule accounts in seconds.[26] Once the

[22] Abhay Raj Singh, 'Digital Payment System in India: Trends, Issues and Challenges' (2025) 6(5) <https://doi.org/10.63363/aijfr.2025.v06i05.1553> accessed 10 September 2026

[23] Emanuel van Praag et al., 'Authorized Push Payment Fraud: Suggestions for the Draft Payment Services Regulation' (2025) 33(5/6) European Review of Private Law <https://kluwerlawonline.com/journalarticle/European+Review+of+Private+Law/33.5/ERPL2025066> accessed 10 September 2026

[24] Aman Pandey and Aishwarya Srivastava, 'Digital Wallets and Mobile Payments: Examining the Legal Risks and Challenges of Financial Frauds in India' (2025) 7(2) IJLSI <https://ijlsi.com/article/view/digital-wallets-and-mobile-payments-examining-the-legal-risks-and-challenges-of-financial-frauds-in-india> accessed 10 September 2026

[25] Ajay Kumar, 'Consumer Protection in the Digital Era: A Critical Analysis of Legal Safeguards against Online Shopping Fraud' (2025) 5(1) Research Review Journal of Social Science <https://doi.org/10.31305/rrjss.2025.v05.n01.026> accessed 10 September 2026

[26] Piyush Mishra, 'Unified Payments Interface (UPI): System Design, Fraud Mechanisms, and Solutions' (2024) Zenodo <https://doi.org/10.5281/zenodo.14062761> accessed 10 September 2026

transaction is made, however, due to the 'singleness of money' concept, it is almost impossible to restore the situation through any real-time measures.[27]

Moreover, the underlying rationale in terms of regulation places the burden of social engineering on the consumer. The banks use 'negligence of customer' as an excuse to avoid compensation on the grounds that the entry of a UPI PIN represents irrefutable evidence of authorisation and consent.[28] This overlooks the fact that there exist psychological attacks in which the 'grooming' of the victim takes place through fraudsters posing as officials from the government or banks. Ultimately, what emerges is a system where the responsibility of the end-user is to pay for any such failure, which could be facilitated by design flaws within the system itself or the inability of the bank to detect obvious mule account activity.

RESEARCH OBJECTIVES

This research aims to:

- Dissect the existing RBI regulations on bank liabilities to assess their relevance to contemporary forms of UPI fraud.[29]
- Role of AI and technology in the gap between detection and redressal to be assessed.[30]
- Identify the legal overlaps between the IT Act, PSS Act, and Consumer Protection Act 2019 to determine the routes of consumer redressal.
- Make a comparison between the liability frameworks in India and best practices abroad, such as the CRM of the UK[31] and the EU's PSD2/PSD3 directives.[32]
- Formulate recommendations on how to ensure harmony between regulation and innovation while protecting consumers.

---

[27] *Annual Economic Report 2022* (Bank for International Settlements, 2022)
[28] Florentina Dani Eti Kusuma Eko Wardani et al., 'Juridical Review of Cyber Security Mobile Banking Digitalization Process For Legal Protection of Customers' (2024) 19(4) Yurisdiksi: Jurnal Wacana Hukum dan Sains <https://doi.org/10.55173/yurisdiksi.v19i4.221> accessed 10 September 2026
[29] *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* (Reserve Bank of India, 2017)
[30] Naga Bhavani Chakkaa and Shaiku Shahida Saheb, 'Mobile payment fraud detection in UPIs through machine learning techniques: A systematic review' (2025) 9(6) Multidisciplinary Reviews <https://doi.org/10.31893/multirev.2026280> accessed 10 September 2026
[31] *Contingent Reimbursement Model* (Lending Standards Board, 2019)
[32] Payment Services in the Internal Market 2015

RESEARCH QUESTIONS

1. In what way is the concept of 'zero and limited liability' by RBI applicable in the case of social engineering in which the customer had entered the UPI PIN through deception?

2. In the case of a breach of security in the UPI platform, how do the obligations of TPAPs differ from those of the banks in question?

3. In what way is the Consumer Protection Act 2019[33] a valid way out for the victims when banks do not take responsibility through RBI circulars?

4. What are the rules for causation, and what evidentiary requirements apply for establishing causation in cases relating to digital payments in India?

5. How could the models for loss allocation be modified to account for 'predictable irrationality' of the consumers in social engineering settings?

RESEARCH METHODOLOGY

The methodology applied in this study is qualitative and doctrinal and is comparative in nature.

Sources of Data: This study uses primary sources of regulations such as RBI Master Directions for Digital Payment Security,[34] NPCI procedural guidelines,[35] and the Integrated Ombudsman Scheme.[36] This is in addition to analysis of statutes under the Payment and Settlement Systems Act 2007, the IT Act 2000 and the Consumer Protection Act 2019.

Secondary Data: A thorough analysis of relevant literature between 2016 and 2026 was done through database searches such as SciSpace and Google Scholar, where the literature is about UPI fraud methods, AI-based security and consumer law.

Analytical Framework: In this study, the PESTLE model (political, economic, social, technological, environmental, and legal) is used to analyse the rise of digital payments and

[33] Consumer Protection Act 2019
[34] *Master Direction on Digital Payment Security Controls* (Reserve Bank of India, 2021)
[35] *UPI Procedural Guidelines* (National Payments Corporation of India)
[36] *Reserve Bank – Integrated Ombudsman Scheme, 2021* (Reserve Bank of India, 2021)

the ABCD (Advantages, Benefits, Constraints, and Disadvantages) Analysis for the evaluation of the UPI system.[37]

Limitations: This research focuses solely on secondary sources and does not include any primary survey data. Judicial precedents analysis will be restricted to the reports available in the literature till early 2026. Technical analysis of the AI models will be done based on their performance from literature reports and not by actually testing them.

ANALYSIS AND DISCUSSION

The UPI Fraud Landscape: From Phishing to Deepfakes: The Indian payment scene has seen an 'alarming' change taking place at 'lightning speed.' The change is from the old practice of queuing up physically to making payments through one's smartphone immediately. Nevertheless, this convenience has led to many different kinds of fraud. A classic form of phishing, where fake sites/messages take away personal information, is frequent.[38] In the case of UPI-based scams, the effectiveness of the QR code scam comes to the fore; the victim is made to scan a QR code that promises him money but ends up debiting his own bank account.

AI's rise has made matters even more complicated. 'Synthetic identity fraud' is one such threat, where deepfake schemes trick the victims into believing the voice or the video belongs to someone they trust. Another type of scam is 'mule accounts,' which are legitimate bank accounts opened by or leased out from vulnerable people.[39] Adaptive malware and screen-sharing software make it possible for the perpetrators to witness the victim key in the UPI PIN, thereby circumventing the security offered by AFA.[40] Normalising small amounts of

[37] Vidya M & Shailashri V, 'A Study on Evolving Digital Transformation in Indian Banking System' (2021) 5(1) International Journal of Case Studies in Business, IT and Education <http://doi.org/10.5281/zenodo.3976932> accessed 10 September 2026

[38] Dian Ekawati et al., 'Phishing in the Banking Sector: Between Cybercrime and Consumer Protection' (2025) 7(1) Sign Jurnal Hukum <https://doi.org/10.37276/sjh.v7i1.422> accessed 10 September 2026

[39] Abhishek Gupta and Hiresh Luhar, 'A Quantitative Study of Fraud Trends in Indian Public Sector Banks: Patterns, Impact, and Prevention' (2025) 15(3) European Economics Letters <https://openurl.ebsco.com/EPDB%3Agcd%3A13%3A14677453/detailv2?sid=ebsco%3Aplink%3Acrawler&id=ebsco%3Agcd%3A189127090&jrnl=23235233&crl=f&link_origin=www.google.com> accessed 30 October 2026

[40] Renuka Kumar et al., 'Security Analysis of Unified Payments Interface and Payment Apps in India' (29th USENIX Security Symposium, Boston, MA, USA2020)

money also ensures that many fraud attempts are never discovered, thus becoming a source of 'volume' income for cybercriminals.

The RBI Liability Framework: The 2017/2019 Directives –

The regulatory policy of the RBI concerning consumer liability mainly revolves around the circular 'Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' (2017),[41] subsequently applied to non-bank prepaid payment instruments (2019).[42]

Zero Liability: If there has been a fraud committed owing to negligence of the bank (e.g., system breach) or a breach by any other third party in which the flaw has been reported within three working days, then there is no liability of the customer.

Limitation of Liability: Provided that the report is lodged within 4 to 7 working days, then the liability of the customer will be limited (for example, ₹5,000 for basic savings account, ₹10,000 for all other savings account and ₹25,000 for credit card).[43]

Full Liability: The key question that arises is that of Customer Negligence. This is an important point that banks make, in that by merely inputting the UPI PIN or the OTP, the customer is negligent irrespective of whether the customer was tricked into doing so.[44] This 'technological authorisation' is considered to be legally binding, and thus leaves the victims of social engineering and APP fraud liable for all. Judicial analysis from other jurisdictions, such as Colombia and Indonesia, shows that banks are supposed to be held responsible 'objectively,' since they are the parties that are profiting from and managing the online interface.

Legal Intersections: IT Act, Consumer Protection, and PSS Act: The Information Technology Act 2000 is the overall law dealing with electronic transactions in India. It deals primarily with the legality of electronic records and responsibilities of 'bodies corporate' in

[41] Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (n 31)
[42] *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Payment Transactions in Prepaid Payment Instruments (PPIs) issued by Authorised Non-banks* (Reserve Bank of India, 2019)
[43] Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (n 31)
[44] Utami (n 16)

maintaining adequate security measures.[45] However, it lacks detailed provisions for frauds associated with fintech innovations such as 'request money' fraud in UPI. Payment and Settlement Systems Act, 2007, enables the RBI to regulate payment systems such as UPI but fails to provide a remedy for individuals under private law.[46]

However, the Consumer Protection Act 2019 presents an alternate approach that is consumer-friendly. In making digital banking a 'service,' consumers can claim compensation for 'deficiency in service.'[47] In such instances, success may depend on the ability of the consumer to establish that the bank did not deliver 'secure, faster, cost-effective' solutions, as was envisioned in the government's digital endeavours.[48] However, the evidentiary standard is still high, and a lot of people are not even aware of such legal protections that are available to them. In this regard, the importance of the Integrated Ombudsman Scheme cannot be underestimated, yet its efficiency is frequently undermined by red tape and the absence of relevant protection for social engineering frauds.[49]

Comparative Lessons and International Models: Worldwide, there is a trend towards 'loss sharing.' The UK mandatory compensation plan for APP frauds is certainly a step away from the 'customer pays' approach.[50] The PSD2 and future PSD3 in the European Union focus on Strong Customer Authentication and mandate that 'gross negligence' be proven by the banks before refusing the refund.[51]

Also, other developing countries are working to improve their systems. Nigeria, for instance, has undergone comparative civil liability analysis that points towards making banks liable for account hacking.[52] The Indonesian regulatory system includes such rules as POJK No.

---

[45] Information Technology Act 2000
[46] Dr Roshan Lal, Rohilla1, 'Legal Issues Involved in Electronic Payments System in India' (2024) 7(2) International Journal of Current Science Research and Review <https://doi.org/10.5281/zenodo.10603940> accessed 10 September 2026
[47] Consumer Protection Act 2019
[48] Neelam Chawla and Basanta Kumar, 'E-Commerce and Consumer Protection in India: The Emerging Trend' (2022) 180(2) Journal of Business Ethics <https://doi.org/10.1007/s10551-021-04884-3> accessed 10 September 2026
[49] Anamika Kadam and Nihal Das, 'UPI and Beyond: Understanding Usage, Security, and Redressal in Digital Payments' (2026) 14(12) <https://doi.org/10.51583/ijltemas.2025.1412000126> accessed 10 September 2026
[50] *Specific Direction 20 (Faster Payments APP Scams Reimbursement Requirement)* (Payment Systems Regulator, 2024)
[51] Payment Services in the Internal Market 2015
[52] Uchenna Jerome Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24(1) Tilburg Law Review <https://doi.org/10.5334/tilr.137> accessed 10 September 2026

12/POJK.03/2018 that underline the bank's obligation to facilitate the digitalisation process. These models seem to indicate that India would do well with an integrated and rights-oriented model that ensures regulation is consistent across fintech and banking institutions.

FINDINGS

Regulatory Disconnect: The present RBI regime views 'authorised' (even if fraudulent) transactions as being the fault of the customer, which leaves a major loophole in protection against social engineering attacks.

Barriers to Evidence: Customers don't have the technological means to produce evidence of third-party breach, while the banking institutions have all the transaction data.

Failure to Address the Problem: The dispute resolution process under the NPCI regime and that of the RBI Ombudsman fail to deliver justice in cases of APP scams since the transaction itself is authorised by the user.

Proliferation of Mule Accounts: Criminals take advantage of the fact that there is no real-time freezing of bank accounts to shift money via mule accounts.

Awareness Gap: Even with efforts such as BE(A)WARE, there is still a problem of poor digital literacy among consumers who do not know about the dangers associated with 'request money' and QR codes.

Third Party App Liability: The TPAPs have been found to avoid liability for any kind of fraud carried out through the platform they use.

RECOMMENDATIONS

Modernise the Definition of Negligence: The RBI needs to issue an updated circular from the one issued in 2017 stating that authorisation through sophisticated social engineering does not absolve banks from liability, especially when there was suspicion in the use of the mule accounts.

Establish a System of Mandatory Reimbursement for APP Fraud: This is an option to make banks and TPAPs liable for APP fraud in order to motivate them to stop such scams from occurring in real time.

Enforce Real-Time AI Monitoring: This will involve mandatory integration of AI monitoring systems, such as MuleHunter.ai, across banks in order to freeze suspicious accounts in real time.

Cooling Off Period: This will be a mandatory delay before any large transaction or a transaction to a new VPA to facilitate cancellation of fraudulent payments.[53]

Strengthen TPAP Accountability: Define the responsibilities of third-party applications under the IT Act and Consumer Protection Act, holding both the platform owner and app provider accountable for any security failure.

National Digital Literacy Mission: Adopt an active approach towards awareness programs, specifically targeting frauds such as QR code frauds and 'Request Money' frauds.

CONCLUSION

The Unified Payments Interface is central to India's future, but its very existence hinges upon having a strong consumer protection regime. The current regulatory and legal approach to dealing with 'unauthorised' transactions leaves a 'liability vacuum' that leaves those affected by social engineering scams bearing the brunt of the consequences. Even as technological advances such as artificial intelligence and behavioural biometric techniques provide some assurance for the future, the regulatory and legal regime must evolve in a manner that places the risk in the hands of those most capable of handling it. In the modern digital age, safeguarding the consumer against fraud and manipulation is fundamental to establishing an inclusive economy.

[53] Nakul Gupta and Dharmender Jhamb, 'How India can develop its payments fraud prevention model: A study of emerging best practices' (2020) 14(3) Journal of Payments Strategy & Systems <https://doi.org/10.69554/ioxt3496> accessed 10 September 2026