CYBER FRAUD IN DIGITAL PAYMENTS: A GLOBAL STUDY ON UPI SCAMS AND ONLINE FINANCIAL CRIMES

Sristy Agrawal, Christ (Deemed to be University), Delhi NCR

ABSTRACT

The convergence of constant availability, low cost of transactions, and designed user interfaces via the real-time and instant payment systems has moved to the limelight of the retail finance to drive mass adoption and inclusion of the financial system. In Brazil, it is the case with Pix and in India, with Unified Payments Interface (UPI), both boasting hundreds of millions of users and having hundreds of millions of transactions within their country, respectively. But, it is the same design features of speed, ubiquity, near irreversibility and low friction pre-transactions that also have also offered fertile grounds to socially engineered and approved push payment (APP)-type fraud that in certain jurisdictions is already surpassing the legacy card fraud.

In this paper, the scams associated with the UPI and other internet financial frauds are discussed through the lens of digital-payment life-cycle and the weaknesses of onboarding, authentication, user interface design, ecosystem governance, and institutional response are identified. It adopts a doctrinal and comparative methodology, which is the reading of statutory and regulatory texts, central-bank circulars, payments-systems books, ombudsman cases, and new case law on UPI fraud in India and the fraud- governance regimes of Pix in Brazil and the Faster Payments system in the new mandatory APP reimbursement regime of the UK.

It is based on the argument that in modern fast-payment fraud, scam-based elements are the primary elements, and are founded upon social engineering, confusion of the UI, mule-account networks, and the inefficiency of redress systems, rather than on any actual technical compromise, and that the current liability systems and redress systems have not yet accommodated an authored-but-induced-transfer paradigm in which card fraud difficulties best suits. The paper proposes a four-pillar regime of rebalancing consumer protection and intermediary responsibility without prioritizing on inclusion or innovation, the four pillars of prevent, detect, respond and recover based on the experiences of other similar countries such as *the Special Return Mechanism (MED)* of Pix and mandatory reimbursement scheme of the UK Payment Systems Regulator. It introduces a systematic typology of UPI frauds, a systematic map of instant-payment fraud protection, and a roadmap of reform to be implemented in UPI- style ecosystems, but customized to other jurisdictions.

Keywords: UPI; fast payments; authorized push payment (APP) fraud; social engineering; mule accounts; cybercrime; consumer protection; dispute resolution.

Introduction

1.1 Background and Rationale

In the last 10 years, the payments environment across the globe has been experiencing a structural sustainability as it moves on to instant account-to-account rails that clear in real time on a 24x7x365 basis, replacing the previous batch and card-based architectures. In India, the leading retail payment tool in 2016 that has been introduced by ***the National Payments Corporation of India (NPCI)*** has become the Unified Payments Interface which currently processes more than 12 billion transactions each month and more than 50 per cent of all real-time transactions in the world.[1] Pix, which was introduced in November 2020 by the Central Bank of Brazil (*Banco Central do Brasil, or BCB*), has also registered almost 150 million users, and around 15 million businesses, becoming the most popular way to pay in the largest economy of Latin America.[2] These systems have common architectural characteristics: openness to multiple banks and payment service providers, addressing using proxies (like the Virtual Payment Address of UPI or Pix keys), the ability to access by QR-codes, and low-cost usage of the system (which encourages mass adoption and high returns in financial inclusion).[3]

However, it is these design features of reduced friction and increased access, which offer space to cyber-enabled financial crime. Data provided in ***the Annual Report of the Reserve Bank of India 2023-2024***[4] and a parliamentary response of February 2024 has been recorded in petitions to the Delhi High Court, which portray a sharp rise in UPI-related fraud losses, which had been around 111 crore in FY 202021 and about 573 crore in FY 202223[5] whilst the total number of cases of digital frauds is reported to have

[1] Sheratt, E. (2024). 'Authorised push payment' bank fraud: What does an effective regulatory response look like? Journal of Financial Regulation, 10(2), 174–200. https://doi.org/10.1093/jfr/fjae009
[2] Sheratt, E. (2024). The view from below: Consumer resistance in authorised push payment fraud. University of Manchester School of Law Working Paper Series. https://research.manchester.ac.uk/en/publications/the-view-from-below
[3] Shum, N. (2025). Authorised push payment fraud: Theorising a loss allocation model. UCL Journal of Law and Jurisprudence, 14(1). https://doi.org/10.14324/111.444.2052-3467.1988
[4] Reserve Bank of India. (2024). Annual Report 2023-2024. RBI. Cited in Pankaj Nigam v. Union of India & Ors., W.P.(C) PIL (Delhi High Court, February 2026).
[5] UK Finance. (2024). Annual Fraud Report 2024. Cited in Sheratt, E. (2024). 'Authorised push payment' bank fraud: What does an effective regulatory response look like? Journal of Financial Regulation, 10(2), 174-200. See also: Payment Systems Regulator. (2025). PS25/5 APP scams reimbursement requirement: Consolidated policy statement. PSR

reached 1.1 million cases in FY 202324 ***In the United Kingdom***[6], a card-fraud loss has been surpassed by authorised push payment (APP) fraud on the Faster Payments system, and the Payment Systems Regulator (PSR) has proposed, which will come into force in October 2024, a compulsory reimbursement regime on victims of APP-fraud. ***In Brazil,***[7] there were also 2.5 million Pix scam cases in 2023, which had a rate of 4.7 scams per minute, even though the average per-transaction fraud rate is low at 0.007 per cent.[8]

This policy issue, then, is that there is a trade-off between the inclusion and effective payment achieved through real-time payments and the increase in cyber-enabled fraud occurrences, in which the victims are duped into authorizing the payment instead of being the victim of a purely technical breach. The traditional models of liability based on the obviously erroneous debit that is manifestly unauthorised find it difficult to adapt to this fact and place the victims in an intermediate place that current regulatory and consumer-protection structures are ill adapted to occupy.[9]

1.2 Research Problem, Objectives and Scope

The particular research problem driving this paper is the proliferation of UPI-related scams, which are authorised but induced, i.e. transactions in which the payer voluntarily sends money, but does so under the pretence, in a system where real-time settlement is enabled and against which card-like holds are ineffective, the time to invalidate and undo a transaction has been radically reduced. The study aims are fourfold: to develop a taxonomy and lifecycle map of UPI-related scams and internet financial crime; to uncover legal, regulatory, and governance gaps in authorisation, authentication, and refund regulations of fast-payment systems; to compare the fast-payment-systems-related fraud controls and consumer-protection frameworks of selected jurisdictions, specifically the Pix in Brazil and the Faster Payments in

[6] Maume, P., Ríos, A., Sánchez, J. L. B., Correia, F., & Panagiotou, A. (2025). Authorised push payment fraud: Suggestions for the draft Payment Services Regulation. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241100

[7] Central Bank of Brazil fraud data (2023). Cited in: Paymentscmi. (2024). How can banks help fight Pix scams? Payments CMI Insights. See also: Commercegate. (2024). Central Bank of Brazil and Febraban to change Pix refund mechanism for fraud victims

[8] Thomas, M., & Mosk, B. (2025). Who pays for payment fraud? Optimal detection and liability rules. Lancaster University Financial Fraud & Money Mules Conference Working Paper, FFMM-057. http://wp.lancs.ac.uk/ffmm2025/files/2025/08/FFMM2025-057-Thomas-Mosk.pdf

[9] Bliss, S. L. (2024). It takes a thief…and a bank: Protecting consumers from fraud and scams on P2P payment platforms. Washington & Lee Law Review (forthcoming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4868009

the UK; and to suggest a reform agenda of covering the prevention, detection, response, and recovery mechanisms of UPI-sets.[10]

The article is concerned with retail-facing fraud, which affects individuals and micro-enterprises, of UPI and similar instant-payment systems, and does not consider corporate treasury operations, or more technical vulnerabilities of wholesale payment infrastructures. The methodology of statutes, regulatory instruments, central-bank circulars, scheme rulebooks, ombudsman decisions and emerging case law is analysed by the doctrinal and comparative methodology. The study is constrained by the incompleteness of the granular, transaction-level frauding information, the secrecy surrounding the PSP-level fraud-management procedures, and the lack of publicly-available decisions on most of the internal or ombudsman-resolvable conflicts. The paper, however, relies on official information in the annual reporting of the RBI, parliamentary responses, petitions submitted by the public interest in Brazil and PSR policy statements in the UK that form the basis of its descriptive and normative analysis.

The paper follows the following structure. ***In Firstly***, the conceptual frameworks, central definitions, as well as the theoretical perspective of UPI fraud are established***.*** ***Secondly*** there is a map of the UPI ecosystem and threat surface and a typology of UPI scams and online financial crime is created. Then aa comparative study of Pix (Brazil) and Faster Payments (UK) is carried out followed by a comparative table. ***Thirdly*** it touches on the legal and regulatory framework in India and incorporates the provisions of the laws and case laws that are relevant. ***Further*** it focuses on institutional response and institutional enforcement. And the framework of the Prevent Detect Respond Recover model is suggested. ***Lastly***, the author sums up and provides recommendations on reform.

Conceptual Foundations, Definitions and Theoretical Lens

2.1 Digital Payments Ecosystem, Actors and Key Concepts

An ecosystem of digital-payments is made up of a variety of layers: payers and payees on the user tier; their banks or non-bank payment service providers (PSPs); the rail or scheme operator, e.g. NPCI in the case of UPI, the Central Bank of Brazil in the case of Pix, or Pay.UK in the case of Faster Payments; front-end apps or aggregators;[11] the telecom and device layers which carry authentication credentials; and financial, data-protection and consumer-protection regulators. Though there is no player visibility of

[10] World Bank Group. (2023). Fraud risks in fast payments (Focus Note). World Bank. https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf

[11] Taavitsainen, N. J. (2025). Trust to exploitation: The legal and societal implications of payment fraud and the path toward stronger protections [Master's thesis, Åbo Akademi University]. https://doria.fi/bitstream/handle/10024/192805/taavitsainen_nanne.pdf.

the full extent of the fraud incident, every layer has a distinct risk factor: SIM-swap threats at the telecom level, credential theft at the device and application level, and an ineffective KYC or transaction monitoring at the banking layer.[12]

Fast-payment systems scheme-based like UPI and Pix are regulated by central rulebooks on participation, settlement, authentication and fraud-management requirements that binding PSPs often leave questions on the liability faced by consumers to national regulation or bilateral contract.[13] In India, an example is ***the Payment and Settlement Systems Act, 2007 (PSS Act)***[14] applying the regulation and supervision of payment systems to only *theReserveBankofIndiaunder**Section3*** and nothing can be done by any other body without prior authorisation by the RBI under ***Section 4. Section 23***[15] of the PSS Act lays down settlement finality, the fact that settlements undertaken using a specified payment system are final and cannot be reversed, which is of direct interest in the issue of reversing fraudulent UPI transacted.[16] This layer of institutionality implies that doctrinal analysis should include rules and regulations of payment systems, banking regulation, consumer protection law and criminal law to formulate a rational structure of liability in cases of fraud.[17]

Fast or instant payments are generally considered to be electronic fund transfers that are sent and cleared in near real-time, around the clock, ***24x7x365,*** with real time or near real time confirmation to both the payer and the payee. In this kind of system, irrevocability of credits, lack of pre-authorisation or chargeback systems[18], which are characteristic of card schemes, create a structural prejudice against ex post dispute resolution. Authorised push payment (**APP**) fraud involves the exposure of the payer to a payment, but he or she, through deception or coercion, as part of an investment, impersonation, or romance scheme, voluntarily makes the payment. Mule accounts Mule accounts are bank or wallet

[12] Gohain, A. (2025). Digital payment frauds in India: A critical analysis of RBI's regulatory framework effectiveness. Indian Journal of Law and Legal Research, 7(2). https://www.ijllr.com/post/digital-payment-frauds-in-india.
[13] European Payments Council. (2023). 2023 payment threats and fraud trends report (EPC181-23 v1.0). European Payments Council. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23
[14] Payment and Settlement Systems Act, 2007 (PSS Act)
Section 3 (Regulation and supervision by RBI): The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, § 3 (India). Available at https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf
[15] id
[16] Gohain, A. (2025). Digital payment frauds in India: A critical analysis of RBI's regulatory framework effectiveness. Indian Journal of Law and Legal Research, 7(2). https://www.ijllr.com/post/digital-payment-frauds-in-india
[17] Kashid, S. (2025). Consumer protection in banking and digital payments in India: Assessing the efficacy of legal and regulatory safeguards in the digital age. International Journal of Advanced Legal Research, 5(2), 1–28. https://ijalr.in/wp-content/uploads/2025/12/Shreya.Kashid_RP_2025.pdf
[18] Section 4 (Authorisation requirement for payment systems): The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, § 4 (India)

accounts, many of which are opened with weak KYC or rented by economically vulnerable people, which can be used as pass-through nodes to launder fraudulent funds quickly and dissipate them to make recovery difficult even in cases where transactions are reported soon.[19]

2.2 Theoretical Lens: Criminology, Behavioural Science and Platform Governance.

The routine-activity theory of criminology is a crime theory that suggests that a crime thrives when motivated offenders are at liberty to find the right target under the absence of the effective guardianship to control them- a three-factor combination that can easily correspond to that of instant-payment ecosystems that have pervasive smartphones, loosely secured accounts, and virtually no real-time controls.[20] The three components of the fraud triangle: opportunity, pressure, and rationalisation also apply to mule-account and merchant-side forms of fraud, as economic susceptibility and the perceived lack of detection provide a consistent stream of middlemen to run scam schemes on a mass scale. Social engineering literature Behavioural Behavioural literature of social engineering exposes how urgency, signs of authority, reciprocity, and fear are being used to avoid rational suspicion in online interaction, and why victims will authorise transactions despite basic transaction information being suspicious.

Platform governance scholarship highlights how intermediaries such as banks, fintech apps, telecom providers and scheme operators influence the risks experienced by design decisions related to the selection to onboard, defaults, friction and information asymmetries which inherently serve de facto regulatory roles. In payments this concurs with regulatory initiatives that impose defined due-diligence and fraud-management obligations on PSPs as in the Pix anti-fraud database and obligatory participation provisions, and the UK in making APP reimbursement and to make costs split between sending and receiving PSPs compulsory.[21] Financial services consumer-protection frameworks are increasingly no longer disclosure-based, but include conduct-of-business, fair-treatment and accessible-redress elements, which can be observed in the recent 2017 directive on customer liability in unauthorised electronic banking transactions in the RBI[22], where customer liability is limited and the onus of proving negligence

[19] Sinha, R. (2025). Phishing in India's fintech era: Liability, enforcement, and consumer protection. International Journal of All Subject Research, 12(11). https://www.allsubjectjournal.com/assets/archives/2025/vol12issue11/12316.pdf
[20] Chatterjee, S., & Rathod, V. (2024). Legal liability for fraud in digital payments. Insurance Times Journal, November 2024. https://bimabazaar.com/journal-books/insurance-times-journal/2024-insurance-times/legal-liability-for-fraud-in-digital-payments
[21] Banerjee, A. (2024). Digital payments in India: Exploring emerging issues in the legal framework. Kozminski University Working Paper Series. https://repozytorium.kozminski.edu.pl/bitstreams/d782a60c-2d96-4138-a562-1207c892b8f1/download
[22] RBI Circular on Customer Protection — Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (6 July 2017)
Reserve Bank of India. (2017, July 6). Customer protection – Limiting liability of customers in unauthorised electronic

on payment issuers increases.[23] A gap in the application of such protections between authorised-but-induced scams and transactions that are plainly non-authorised, however, persists in the literature, and is the topic of this paper in the case of UPI and similar instant-payment rails.

UPI Ecosystem, Threat Surface and Typology of Scams

3.1 UPI Architecture and Points of Failure

UPI is an API-based, instant-payment system, and multi-bank system, where individuals can connect multiple bank accounts to one Virtual Payment Address (**VPA**), QR code or mobile number, allowing a push and a collect flow and real-time settlement provided by the central switch of **NPCI.** Such architecture, overlaid with no or minimal user level fees and a strong integration with daily life applications via third-party PSP applications like PhonePe, Google Pay and Paytm has elevated UPI to be the default tool of peer-to-peer and small-value merchant payments in India.[24] To scammers, the ubiquitousness, low friction and absence of pre-authorisation of UPI combine to generate high liquidity and fast money transfers which can be leveraged in phishing, fake customer-support calls and payments misdirected, particularly in situations with low user awareness and a low level of device protection.[25]

Failures of the UPI ecosystem occur on various levels. During the onboarding, the mules of the accounts are created by using erudite KYC or synthetic identities. SIM-swap attacks are also made possible in the telecom layer,[26] through which OTP can be intercepted, which was the subject of the Supreme Court of India multi-bank UPI fraud advisory reference of 2020 (***RBI v. NPCI & Bank, 2020)***[27], emphasizing the need to use two-factor authentication and monitor it in real time. At the machine level, viruses and remote access applications steal UPI PINs and approve transactions without the real permission of the

banking transactions (Circular No. RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18). https://taxguru.in/rbi/customer-protection-limiting-liability-customers-unauthorised-electronic-banking-transactions.html

[23] Sheratt, E. (2024). 'Authorised push payment' bank fraud: What does an effective regulatory response look like? Journal of Financial Regulation, 10(2), 174–200. https://doi.org/10.1093/jfr/fjae009

[24] Maume, P., Ríos, A., Sánchez, J. L. B., Correia, F., & Panagiotou, A. (2025). Authorised push payment fraud: Suggestions for the draft Payment Services Regulation. SSRN Electronic Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241100

[25] Shum, N. (2025). Authorised push payment fraud: Theorising a loss allocation model. UCL Journal of Law and Jurisprudence, 14(1). https://doi.org/10.14324/111.444.2052-3467.1988

[26] Pratt, T. C., & Turanovic, J. J. (2025). The effects of risky behaviours and social factors on the frequency of mass marketing fraud victimisation: A routine activity theory approach. Innovation in Aging, 9(2), igae111. https://doi.org/10.1093/geroni/igae111

[27] RBI v. NPCI & Bank — Advisory Reference (2020, Supreme Court of India)
RBI v. NPCI & Bank, Supreme Court of India, Advisory Reference (2020). NPCI is a facilitator; banks are directly liable for customer losses; two-factor authentication, timely dispute resolution, and real-time fraud monitoring are essential.

user. In the area of UI/UX design,[28] the confusion of request flows of collecting and paying, misleading prompts, and disguised payment links take advantage of cognitive heuristics to provoke their victims to authorise outgoing transfers under the belief that they are being offered money. In **February 2026**, an advocacy filed by ***Pankaj Nigam in the Delhi High Court***,[29] noted the fraud cases are on the rise, the KYC standards are not uniform, there is no single window mechanism of complaints and the methods of preserving the metadata of transactions are inadequate as factors to reduce effective guardians and lagging of the freeze of the suspected funds

3.2 Typology of UPI Scams and Online Financial Crimes

The UPI-based fraud and web-based financial crimes which might refer to them can be classified into four broad types in which every form of scam denotes an alternative vulnerability within the payment lifecycle.[30]

The most common and prevalent type of scams is social-engineering and APP-style scam, which encompasses deception into fake KYC-update or **RBI/NPCI** messages, reward or refund bait (the promise of winnings or cashback), a collect request scam (where the scammer tricks a victim into authorising pull request on the pretext of sending money) and fake customer-support impersonation scam (where the scammer impersonates a bank or app help-desk operator and gets a victim to provide OTPs, install remote-access These frauds replicate trends in APP fraud in the UK, where people are swindled regarding the nature or the identity of payments, and where the distinction between what is authorised and not is legally disputed regardless of obvious social engineering.. In ***Kotak Mahindra Bank v. Ramesh Sharma (2021,*** The court, Bombay high court[31], ruled that a bank should maintain high levels of security and it is obligatory to educate its customers on phishing and that a bank should not deny reimbursement to a person on the grounds of so-called negligence of the customer.

To intercept OTPs, install malware or remote-access software, steal credentials by use of phishing websites or fake UPI applications that resemble professional interfaces, are all forms of technical-compromise attacks. In the ***HDFC Bank v. Customer – UPI OTP Hijacking matter*** (2022, Delhi

[28] Information Technology Act, 2000 (as amended 2008)
Section 43 (Penalty and compensation for damage to computer system): The Information Technology Act, 2000, No. 21, Acts of Parliament, § 43 (India). Available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[29] Holt, T. J., & Bossler, A. M. (2015). An application of routine activities theory to online identity theft. British Journal of Criminology, 56(1), 21–37. https://doi.org/10.1093/bjc/azv011
[30] Hare Ram Singh v. Reserve Bank of India & Ors., W.P.(C) 13497/2022 (Delhi High Court, decided 18 November 2024, per Dharmesh Sharma, J.)
[31] Kotak Mahindra Bank v. Ramesh Sharma, 2021 SCC OnLine Bom (Bombay High Court)

District Consumer Forum)[32], the forum stated that there is no evidentiary basis to hold banks liable in cases where there is no evidence of negligence on part of customers in case of OTPs hijacking, and added that the UPI guidelines provided by RBI mandated that banks would compensate customers against unauthorised debits.

The spectrum of merchant and market fraud includes scams like counterfeit e-commerce posts and replacing QR-codes on physical points-of-sale to scams involving delivery-related payment-links where the victims make purchases that are not delivered.

Organised fraud networks are based on mule-account infrastructures of a large scale. According to what is recorded in Brazil, Pix scam proceeds are moved very fast on many accounts with very low balances when Special Return Mechanism (**MED**) is activated. Multi-bank UPI frauds have similar layers and quick forward transfers and Indian courts have highlighted the responsibilities of banks to observe and the position of NPCI as facilitator of the scheme, and affirmed the responsibility of account-holding banks to customers as the main liability.

Comparative Global Study: Pix (Brazil) and Faster Payments (UK)

4.1 Brazil's Pix: Design, Security Architecture and the Special Return Mechanism

Pix, released by ***the Central Bank of Brazil*** in November 2020[33], is an account-to-account, centralised instant-payment system, which is a part of the national financial infrastructure (SPI), with proxy identifiers (Pix keys), interoperable QR codes, and 24x7 real-time settlement.[34] Since its creation, the incorporation of security features into the BCB[35] as a proactive measure in fraud control, includes transaction restrictions (particularly lower amounts during off-peak hours), preventive blocks on suspicious transfers, centralised anti-fraud database to flag high-risk accounts and devices,[36] and the

[32] HDFC Bank v. Customer (UPI OTP Hijacking), 2022 SCC OnLine (Delhi District Consumer Disputes Redressal Forum)
[33] International Monetary Fund. (2023). Pix: Brazil's successful instant payment system. IMF Country Report No. 2023/289,
[34] Sacramento, P. (2026). Privacy as infrastructure: What Brazil's Pix teaches the world. SSRN Electronic Journal (Version 1). https://www.psacramento.com/privacy-as-infrastructure-what-brazils-pix-teaches-the-world/
[35] Bank for International Settlements. (2021). Lessons from Brazil's Pix (Online Appendix). BIS Bulletin No. 52. https://www.bis.org/publ/bisbull52_appendix.pdf
[36] Alvares, J. (2025). The political economy of Brazil's Pix payment system. ProMarket (Stigler Center, University of Chicago Booth School of Business). https://www.promarket.org/2025/12/03/the-political-economy-of-brazils-pix-payment-system/

Special Return Mechanism (***Mecanismo Especial de Devolução, or MED***) to allow quick refunds on fraud and operational malfunctions.[37]

The MED enables the victims of fraud to complain to their financial institution within the next 80 days after the transfer of Pix. When it is notified, the funds are frozen in the account of the recipient awaiting scrutiny. In case of fraud, money is refunded to the victim, however, this depends on the availability of funds in the account of the fraudster by the time when the blocking is carried out.[38] Practically, the MED has also not been effective: in 2023, it reimbursed a significantly lower proportion of requested amount in refund, approximately 9 per cent, due in part because scammers withdraw funds out of the first receiving account before block execution is possible, and in part because layering continues to use many mule accounts in a few minutes. To combat this, the BCB has come up with MED 2.0 that will be a requirement to all the Pix-participating institutions by February of 2026. MED 2.0 also allows one to trace and block funds on more than one account (more than a single layer up the fraud chain), instead of a single account that initially receives the money, and hence, it becomes much harder to conceal the proceeds by redistributing money again. Moreover, in October 2025 the BCB introduced a self-service dispute button which means that Pix users will be able to initiate a blockage of funds straight to their banking apps, with a structured timeline: once they are notified of a dispute, immediately the recipient bank must block disputed funds, both banks will have seven days to view the dispute, and in case of fraud confirmed the payment is returned within eleven days.[39]

Other compliance strategies have been ***the BCB Resolution No. 506 (September 2024)***, which strengthened the security requirements of Pix participants and Resolution No. 507, which established a new penalties manual in case of non-compliance. The BCB also introduced tougher entry requirements to participate in Pix, stronger anti-fraud database reporting and required all participating institutions to provide a direct in-app channel on which users could open, track, and manage dispute claims.

[37] Brandt, C. E. (2024). Pix: The latest updates on Brazil's leading instant payment scheme [Interview]. European Payments Council Insights. https://www.europeanpaymentscouncil.eu/news-insights/insight/pix-latest-updates-brazils-leading-instant-payment-scheme

[38] Reserve Bank Innovation Hub. (2024). Mule accounts: Leveraging AI/ML for proactive detection (RBIH Whitepaper). Reserve Bank Innovation Hub, Reserve Bank of India. https://rbihub.in/wp-content/uploads/2024/07/RBIH-Whitepaper_Mule-Accounts.pdf

[39] Indian School of Business, Institute of Data Science. (2024). Mule account identification and detection using machine learning models (IDS Research Paper). https://www.isb.edu/faculty-and-research/isb-institute-of-data-science/research/mule-account-identification-and-detection-using-ml-models

Nonetheless, due to these efforts, the amount of Pix is still significant, and the inherent issue of inter-institutional coordination and speed-of-blocking does not have a solution.[40]

4.2 UK Faster Payments: Mandatory APP-Fraud Reimbursement and Liability Architecture

Faster Payments system of Pay.[41]UK which operates in the United Kingdom has seen a strong increase in APP fraud, to the point where it now surpasses card-fraud losses and is the focus of a compulsory reimbursement regime introduced by ***the Payment Systems Regulator (PSR)*** effective 7 October 2024[42]. Section 72 of the Financial Services and Markets Act 2023 which was granted Royal Assent on 29 June 2023 formed legal foundation to this regime and required the payments order to be made by the PSR under the Faster Payments Scheme to become law (mandatory) to be reimbursed by the APP.[43] The regime is effected using three legal tools which are ***Specific Requirement 1 (SR1***), which requires Pay.UK to incorporate the reimbursement requirement into FPS rules, ***Specific Direction 20 (SD20)***, which requires in-scope PSPs to comply with the reimbursement rules, and ***Specific Direction 19 (SD19)***, imposing a requirement on Pay.UK to have an effective compliance monitoring regime.[44]

The main provisions of UK APP-fraud reimbursement regime include the following. The sending **PSP** will have to compensate all its eligible customers that is consumers, micro-enterprise, and charities against APP fraud, to the maximum of **£85,000** per claim and no minimum is specified. Reimbursement costs are equally divided between the sending and receiving PSPs creating a 50/50 incentive on both sides of the transaction to invest in fraud prevention and detection. Reimbursement is to be given within five business days, [45]subject to a so-called stop the clock option of giving more time to investigate it, and the final decision is to be made within 35 business days. PSPs can make a voluntary surplus up to a maximum of **£100** and the claims should be reported within ***13 months*** of the date of the last payment related to it. More importantly, the fraudulent acts of the first party (customer is fraudulent) and gross

[40] University of Central Lancashire. (2024). Money mules: Understanding the role of money mule networks in facilitating cybercrime (Lancashire Cybercrime Research Whitepaper). https://knowledge.lancashire.ac.uk/id/eprint/55295/1/Money%20Mules%20Report%202024%20(1).pdf[8]
[41] Financial Conduct Authority. (2025). Proceeds of fraud: Detecting and preventing money mules (Multi-Firm Review). FCA. https://www.fca.org.uk/publications/multi-firm-reviews/proceeds-fraud-detecting-preventing-money-mules
[42] Sheratt, E. (2024). 'Authorised push payment' bank fraud: What does an effective regulatory response look like? Journal of Financial Regulation, 10(2), 174–200. https://doi.org/10.1093/jfr/fjae009
[43] Orritt, G., & Murphy, D. (2026). Moving to mandatory reimbursement for APP fraud. Compliance Monitor (Informa Law / i-law). https://www.i-law.com/ilaw/doc/view.htm?id=436502
[44] World Bank Group. (2023). Fraud risks in fast payments (Focus Note). World Bank. https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf
[45] Bird & Bird LLP. (2023). What are the latest developments in relation to the new mandatory reimbursement scheme for APP fraud? Bird & Bird Fintech Newsletter, December 2023. https://www.twobirds.com/en/insights/2023/uk/what-are-the-latest-developments-in-relation-to-the-new-mandatory-reimbursement-scheme

negligence are the only reasons that should justify refusing reimbursement, and the latter is construed by the PSR to be higher standards than that which the ordinary person ought to exercise under the common law, and the consumer must have shown a very high standard of negligence, which is found to be higher than ordinary negligence.[46] The consumer standard of caution is not applied to the vulnerable customers, and the excess on the claim is not available.

Active prevention is also an ingredient in the regime. ***The Payment Services (Amendment) Regulations 2024, effective 30 October 2024,***[47] enable PSPs to postpone the implementation of a suspect payment of up to four business days (**D+4**)[48] where there are reasonable causes to believe a fraud or dishonesty[49], which is more lenient than the previous **D+1.** The PSR recommends that the advice on consumer communications needs to be product-specific, as well as consumer- and scam-specific and transaction-specific, and needs to be non-boilerplate. PSPs are supposed to implement confirmation-of-payee systems, enhanced onboarding, and transaction-monitoring systems as well as to freeze or stop suspicious payments. The reporting system is facilitated with the regime, that requires monthly data submission on APP-fraud claims, published by the PSR to generate transparency and reputational incentives.[50]

Another comparator is found in Singapore. ***The Shared Responsibility Framework*** (**SRF**) was implemented by ***the Monetary Authority of Singapore (MAS)*** and ***Infocomm Media Development Authority (IMDA)*** effective as of December 2024 and is applied in unauthorised payment transactions in the event of a phishing attack.[51] Under the **SRF**, the articles of responsible financial institutions and telecoms require that they meet certain requirements e.g., a 12-hour cooling-off period on new devices, notification of transactions in real-time, 24/7 reporting frameworks with a consumer kill-switch, and real-

[46] Hogan Lovells LLP. (2024). UK APP fraud: What in-scope PSPs need to know about the new mandatory reimbursement regime. Hogan Lovells Engage, October 2024. https://www.hoganlovells.com/en/publications/uk-app-fraud-what-in-scope-psps-need-to-know-about-the-new-mandatory-reimbursement-regime

[47] Payment Systems Regulator. (2025). PS25/5 APP scams reimbursement requirement: Consolidated policy statement (May 2025). PSR. https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf

[48] Farrer & Co. (2024). Authorised push payment fraud and mandatory reimbursement. Farrer & Co Insights, October 2024. https://www.farrer.co.uk/news-and-insights/authorised-push-payment-fraud-and-mandatory-reimbursement/

[49] Freshfields Bruckhaus Deringer LLP. (2024). Authorised push payment fraud: A new mandatory reimbursement regime. Freshfields Insights, November 2024. https://www.freshfields.com/en/our-thinking/briefings/2024/09/authorised-push-payment-fraud-a-new-mandatory-reimbursement-regime

[50] HM Treasury. (2024). The Payment Services (Amendment) Regulations 2024: Policy note. UK Government. https://assets.publishing.service.gov.uk/media/65eed7233649a26deded630f/Policy_note.pdf

[51] Singapore Shared Responsibility Framework and Protection from Scams Bill
Monetary Authority of Singapore & Infocomm Media Development Authority. (2024). Guidelines on Shared Responsibility Framework. MAS. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

time fraud monitoring or face liability in the event of a full consumer loss through a waterfall approach, such that the financial institution bears the loss first, then the telco bears the loss. Singapore has also passed ***the Protection from Scams Bill (January 2025),*** which allows police to impose Restriction Orders to banks to limit the banking activities of an individual to at least 30 days in cases of reasonable belief that the individual is a victim of scam.[52]

Comparative Summary: UPI, Pix and Faster Payments

Feature	**UPI (India)**	**Pix (Brazil)**	**Faster Payments (UK)**
Settlement	Real-time 24x7 via NPCI switch	Real-time 24x7 via central bank SPI	Real-time or near-real-time via FPS
Consumer liability baseline	RBI 2017 circular limits liability in unauthorised e-transactions; burden on bank; APP-fraud treatment evolving	MED enables refunds for fraud but low recovery (~9% of amounts in 2023); MED 2.0 mandated from February 2026	Mandatory APP-fraud reimbursement up to £85,000; cost split 50-50 between PSPs; exceptions only for fraud or gross negligence
Dispute/freeze tools	Cybercrime helpline 1930, cybercrime.gov.in portal; coordination challenges; judicial scrutiny via PIL	MED, MED 2.0 (multi-layer tracing), in-app dispute button	Power to delay suspect payments by D+4; bespoke warnings; post-fraud mandatory reimbursemen
Key legislation	PSS Act, 2007; IT Act, 2000 (as amended 2008); BNS, 2023; RBI circulars	BCB Pix regulations; Resolution 506 and 507 (2024); MED rules	Financial Services and Markets Act 2023, s.72; Payment Services Regulations 2017 (as amended 2024); PSR Directions SD19, SD20, SD21

[52] Goh, E. H., & Tok, N. (2024). Singapore to implement Shared Responsibility Framework for phishing scams. Reed Smith Client Alerts, October 2024. https://www.reedsmith.com/en/perspectives/2024/11/singapore-to-implement-shared-

Legal and Regulatory Analysis: India and Cross-Cutting Issues

5.1 Statutory Framework and Relevant Case Law

The legal reaction of India to the digital-payment fraud falls within various fields: criminal law, regulation of the payment systems, banking regulation, and consumer-protection law. It has since been codified in ***the Bharatiya Nyaya Sanhita, 2023 (BNS)***[53] (hereinafter) to replace ***the Indian Penal Code, 1860***[54], effective 1 July 2024. **Section 318(1)**[55] BNS defines cheating as known as fraudulently or dishonestly causing any individual to deliver property, whereas **Section 318(4)**[56] provides penalty of maximum seven years imprisonment and fine on cheating that maliciously results to delivery of property or alteration of a significant security. S**ection 319 BNS**[57] addresses cheating through personation, which directly applies to the impersonation-based UPI scams and the punishment goes up to five year imprisonment. **Section 336(3) BNS**[58] deals with the intentional forgery that is treated with a jail term of up to seven years and fine and **Section 340(2)**[59] deals with the abuse of a forged electronic record as true. The expanded scope of movable property in the BNS has now expanded to include movable property in the form of intangible property and, therefore, theft of data and thus theft of online information through hacking bank accounts or cloning equipment is not left out in the provision of **Section 303 BNS**.[60]

Cyber-offences have specific provisions given by ***the Information Technology Act, 2000*** (which was amended in 2008)[61]. **Section 43**[62] deals with the unauthorised access or damage to the computer systems,

[53] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament (India)
[54] the Indian Penal Code, 1860. Published in the Gazette of India, Extraordinary, Part II, Section 1. Available at https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf.
[55] Section 318(1) (Cheating — fraudulently or dishonestly inducing delivery of property): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 318(1) (India).
[56] Section 318(4) (Cheating — dishonestly inducing delivery of property or alteration of valuable security; imprisonment up to 7 years and fine): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 318(4) (India) .
[57] Section 319 (Cheating by personation; imprisonment up to 5 years): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 319 (India) .
[58] Section 336(3) (Forgery with intent to cheat; imprisonment up to 7 years and fine): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 336(3) (India) .
[59] Section 340(2) (Using forged electronic record as genuine): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 340(2) (India) .
[60] Section 303 (Theft, including intangible property and data): The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, § 303 (India). Available at https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
[61] Information Technology Act, 2000 (as amended 2008)
[62] Section 43 (Penalty and compensation for unauthorised access/damage to computer system): The Information Technology Act, 2000, No. 21, Acts of Parliament, § 43 (India). Available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

and the respective parties are entitled to compensation. **Section 66** imposes a prison sentence of up to three years or 5 lakh rupees fine as punishment on hacking. ***Section 66C*** [63]is a provision that specifies punishment of identity theft-i.e. using electronic signature or password or a unique identification feature of the other person- with imprisonment of up to three years and a fine of 1 lakh rupees. Section 66D[64] [65]deals with cheating through personation by using a computer resource with a penalties of imprisonment up to three years and fine up to 100 lakh. These clauses directly relate to UPI-fraud cases that touch on phishing, identity theft, and impersonation by a fake application.

The regulatory layer of the payment system is ***the payment and settlement systems act of 2007 (PSS Act)***. **Section 4** stipulates that RBI must approve all the payment system operators and that they must comply with safety, security, and operational standards. Section 6 also gives the RBI the power to give guidelines to the operators of payment systems about the guidelines to operate, redressing of consumer grievances and cybersecurity. Section 10 allows payment system inspection and supervision by RBI. **Section 23** defines settlement finality of settlements by specified systems final and irrevocable, which, although safeguarding systemic integrity, poses the very challenge of reversing the post-settlement fraud recovery so hard in UPI. Section 26 includes sanctions against the operators in the event of breach of the law such as working without permission.

The circular issued by the RBI of 6 July 2017,[66] which was named Customer Protection-Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. (*RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18)*[67], is the underlying regulatory tool of consumer liability of electronic payment fraud.[68] The circular obliges banks to develop strong and dynamic fraud detection and prevention systems, the real-time alert on all electronical transactions, and develop avenues that

[63] Section 66C (Identity theft — using another's electronic signature, password, or unique identification; imprisonment up to 3 years and fine up to ₹1 lakh): The Information Technology Act, 2000, No. 21, Acts of Parliament, § 66C (India)
[64] Section 66D (Cheating by personation using computer resource; imprisonment up to 3 years and fine up to ₹1 lakh): The Information Technology Act, 2000, No. 21, Acts of Parliament, § 66D (India)
[65]Section 4 (Authorisation for operating payment systems — prior RBI approval mandatory): The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, § 4 (India). Available at https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf
[66] Section 6 (Power of RBI to issue directions to payment system operators on operational guidelines, consumer grievance redressal, and cybersecurity): The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, § 6 (India)
[67] RBI Circular dated 6 July 2017 — Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions
(Circular No. RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18)
Clause 4: Banks must establish robust and dynamic fraud detection and prevention mechanisms.
[68] Section 10 (Inspection and oversight of payment systems by RBI): The Payment and Settlement Systems Act, 2007, No. 51, Acts of Parliament, § 10 (India)

allow reporting of unauthorised transactions. Clause 8 is that in the case of the loss caused by the breach of the third-party, and there is no negligence of the customer or the bank, no customer liability is received in case the customer informs the bank within three working days. In case it is reported by the customer within four-seven working days, the liability limit is limited to 10,000 rupees in case of basic savings and 25,000 rupees in the other account depending on the type of transaction. It is up to the bank to bear the burden of establishing the negligence of customers. The Allahabad High Court recently reiterated this ***Suresh Chandra Singh Negi v. Bank of Baroda (2025)***[69], and that a Division Bench of Justice Shekhar B. Saraf and Justice Praveen Kumar Giri decided: A critical reading of the above circular would reveal that the onus of proving the liability of the customer in the event of unauthorized electronic banking is on the bank.

The Consumer Protection Act, 2019,[70] provides the consumer-protection layer with the express inclusion of e-commerce transactions as well as the definition of unfair trade practice under **Section 2(47)** including the provision of deceptive or manipulative action through the use of electronic records. The Act gives powers to ***Central Consumer Protection Authority (CCPA)*** to investigate[71], bring complaints and take measures against unfair trade practices, misleading practices. It requires e-commerce service providers to develop grievance redressal schemes in a month of time and has provided a product liability to hold manufacturers, service providers and sellers liable to defective products and services. **Section 2(42)** on unfair contract also shields the consumer against any unseen costs or conditions that are disproportionately favorable to the service provider.

There are five historic judicial and quasi- judicial cases that have influenced the liability situation in the UPI-specific context:

1. ***State Bank of India v. Ravi Kumar (2019, Delhi High Court):***[72] The SBI UPI account of the victim was hacked and money wired to various accounts unknown to this individual. It was ruled that banks bear the primary responsibility in making sure that the UPI transactions are safe and that any unauthorised debits that occur as a result of vulnerabilities in the systems or negligence

[69] Suresh Chandra Singh Negi v. Bank of Baroda, 2025 SCC OnLine All 115460 (Allahabad High Court, Division Bench: Shekhar B. Saraf and Praveen Kumar Giri, JJ.)
[70] Section 2(42) (Definition of "unfair contract" — terms causing significant change in rights of consumers): The Consumer Protection Act, 2019, No. 35, Acts of Parliament, § 2(42) (India). Available at https://ncdrc.nic.in/bare_acts/CPA2019.pdf
[71] Section 2(47) (Definition of "unfair trade practice" — including deceptive or manipulative conduct through electronic records): The Consumer Protection Act, 2019, No. 35, Acts of Parliament, § 2(47) (India)
[72] State Bank of India v. Ravi Kumar, W.P.(C) (Delhi High Court, 2019)

on the part of the banks should be reversed. The ruling solidified the appropriateness of the customer grievance redressal and reimbursement principles of RBI to UPI fraudulent activity.

2. ***ICICI Bank v. Consumer Forum (2019, NCDRC):*** One of the customers, having ICICI UPI account, was compromised and money was withdrawn through spam UPI applications. The NCDRC decided that banks should pay the customer any loss caused by the UPI fraud in the absence of the loss caused by negligence on the part of the customer (such as by voluntarily providing the UPI PIN), and that secure authentication measures and adequate monitoring of transactions are the mandate of the banks.

3. ***RBI v. NPCI & Bank (2020, Supreme Court Advisory Reference):*** One of the massive frauds had involved a series of UPI transactions with various banks by SIM-swap methods. The Supreme Court stressed that NPCI is just a facilitator with the banks directly liable in the event of any losses to the customers, insisted on a 2-factor authentication, timely redressing the dispute, and real-time monitoring and fraud risk management procedures, and mandated guidelines to follow.

4. ***Kotak Mahindra Bank v. Ramesh Sharma (2021, Bombay High Court):*** The UPI ID of a customer was stolen through phishing and money stolen. The bank would not reimburse money alleging negligence among customers. The court concluded that banks have to possess effective security systems and should educate their customers about phishing, and that in case the bank did not realize that a suspicious transaction was made, it could not deny reimbursement based on the claim of negligence on their part.

5. ***HDFC Bank v. Customer – UPI OTP Hijacking (2022, Delhi District Consumer Forum):*** The account interceptors received the OTPs dispatched to the customer on his phone and moved the money using UPI. The forum stated that the banks are liable in case of no clear evidence of negligence by the customer, restated that the UPI regulations of RBI obliges the banks to give compensation to customers who had been defrauded, and the importance of alert in real time, transaction monitoring, and fraud investigation procedures was pointed out.

5.2 Doctrinal Gaps: APP Fraud, Intermediary Responsibilities and Data Sharing

One of the major inconsistencies in the Indian structure is the treatment of authorised yet induced transactions. The 2017 circular issued by the RBI and the court rulings mentioned above are rooted on

the idea behind the unauthorised electronic banking transactions in cases where the customer did not even want to complete the payment. However, in APP-style frauds, the customer did approve the transaction, either by entering their UPI PIN or by allowing someone to collect it, but he or she did so with misrepresentation. The circular does not specifically cover this category and the terms and conditions of banks usually discuss any transaction authenticated by the PIN of the customer as being authorised, leaving victims of APP-fraud with no direct way to take action in the limited-liability framework. This is in sharp juxtaposition with the explicit UK mandatory reimbursement model in APP fraud based on the assumption that there is reimbursement in the absence of gross negligence, and the MED process in Brazil, which is eventuated by reported fraud irrespective of whether the customer technically authorised the Pix transfer.

The mediator roles should also be recalibrated. Although banks and PSPs have direct responsibilities in authentication and surveillance, telecommunication operators regulate the issuance of SIM cards and the overall network protection, and the provider of apps determine the appearance of the UI/UX and in-app warnings about scams, however, there is no integrated structure of data-sharing and collective prevention that aligns with the privacy standards. Furthermore, this is specifically demanded by the PIL of the Delhi High Court dated February 2026, which wants to provide an exclusive, combined platform connecting the National Cyber Crime Portal to UPI apps, banks, PSPs and telecom operators and a mandatory log of detailed transactions and metadata. Here Singapore has its ***Shared Responsibility Framework*** (SRF):[73] it sets essential duties of financial institutions and telecoms, with a waterfall of liability, in which case the financial institution is initially liable, followed by the telco, and finally the consumer, but the intermediaries must both have discharged their obligations before the loss is handed over. Future data protection and cybersecurity policy in India such as the Digital Personal Data Protection Act, 2023[74] must balance between safe and proportional fraud-intelligence sharing, as in the centralized anti-fraud database of Pix, and prevent excessive surveillance.[75]

[73] RBI Circular dated 6 July 2017 — Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions
(Circular No. RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18)

[74] Digital Personal Data Protection Act, 2023 (DPDP Act)
The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament (India). See also: Gauba, R. (2025). A critical analysis of India's DPDP Act, 2023. Law, Digital Technologies and Artificial Intelligence (LDTA), HSE University. https://lida.hse.ru/article/view/27529; Mishra, S. (2025). The Digital Personal Data Protection Act, 2023 — A legal analysis. International Journal of Law, 11(3), 126–

[75] Global Anti-Scam Alliance. (2025). Singapore's Shared Responsibility Framework: A global model for combating phishing scams. GASA Insights, January 2025. https://www.gasa.org/post/singapore-s-shared-responsibility-framework-a-global-model-for-combating-phishing-scams

Institutional Response and Enforcement

6.1 India' s Reporting Architecture and Operational Challenges

India has put in place a multi-level reporting system on cyber fraud: the national cyber-crime helpline (1930), the cybercrime.gov.in portal, bank-level complaint hotlines, and app-level complaint ports of UPI PSPs. Indian Cyber Crime Coordination Centre (I4C), which is under the ministry of home affairs, liaises with state police cyber cells, banks and payment intermediaries. Nevertheless, applicants to the Delhi High Court argue that this multi window architecture adds delays and delays freezing of fraudulent UPI transactions in time especially where a scam cuts across more than a single bank and jurisdiction. The PIL aims at the establishment of a single and integrated platform of complaint and tracking system directly connected with UPI applications, banks, payment service providers, telecommunication services and law enforcement agencies and the obligatory standard operating procedures to preserve evidence and freeze funds.[76]

The petition also challenges the efficiency of the current redressal process of NPCI UPI dispute resolution system because, the system classifies the complaints under established heads and fails to give a real-time access to vital details of the transaction like bank account details of the recipient. It accuses it of not having clear recognition and tracking mechanisms to complainants, and questions the issue of anonymity in peer-to-peer UPI transfers, which prevents the investigative agencies to access transaction logs and account information as soon as its needed. Others such as operational issues, which comprise mule account proliferation, where nominal account-holders are in most cases economic vulnerable people gained by organised networks, cross-state and cross-border factors in proceeds of fraud (especially when money is exchanged into cryptocurrency or sent abroad), and jurisdiction clashes with state police, central agencies, and the banking regulator are also challenged.

6.2 Comparative Institutional Responses: Pix, UK and Singapore

The strategy of Brazil incorporates reporting and containment in the payment infrastructure itself. The new dispute-button mechanism and the MED enable the users to block the funds directly on their banking apps, giving a specified time frame on the investigation and resolution.[77] The multi-layer tracing feature of MED 2.0, which allows blocking of funds in the chain of fraud victims, not only the initial one,

[76] Allen & Overy Shearman Sterling LLP. (2025). Combatting payment account fraud: Singapore's Shared Responsibility Framework. A&O Shearman Insights, January 2025. https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/combatting-payment-account-fraud-singapores-shared-responsibility-framework

[77] Monetary Authority of Singapore & Infocomm Media Development Authority. (2024). Guidelines on Shared Responsibility Framework. MAS. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

but also solves the main operational problem of the quick disappearance of funds. Nonetheless, even MED, refunds are frequently unsuccessful since scammer accounts get emptied before blocks can be executed in 2023, only approximately 35 per cent of successful MED refunds compensated the full value of the reported scam.[78]

The UK regime focuses on post-fraud reimbursement on the basis of set timeframes and cost sharing. The PSR will present the monthly submissions of APP-fraud claims data, which will be published to provide transparency and reputational enhancement to PSPs to invest in fraud prevention. The offering of a real-time intervention tool: The authority to suspend payments made by the suspect up to four business days by the Payment Services (Amendment) Regulations 2024 is an operational tool. The external dispute-resolution body is ***the Financial Ombudsman Service (FOS),*** which has the authority to give compensation of up to 430,000 per complaint, which is a strong accountability tool against PSPs that reject valid claims of reimbursement.[79]

Singapore SRF operationalises a four-stage claim process, namely claim, investigation (2145 business days), outcome and recourse, and ***the Financial Industry Disputes Resolution Centre (FIDReC)*** can be used as an external review body. The Protection from Scams Bill should introduce a new real-time intervention tool: a police-imposed Restriction Orders, which may freeze the banking activities of a potential victim up to 30 days, and may be renewed up to five times, which is designed as a last resort to respond to those who refuse to believe that they become a victim of scam.Institutional response metrics should not be limited to a number of raw complaints, but should include average times-to-freeze, percentage of money successfully recovered, timelines of in response, and repeat-victimisation rates, as well as The compilation and publication of such metrics - in the UK like the PSR does[80] - establishes regulatory and reputational incentives to systemic improvement.

Recommendations and Model Framework: Prevent–Detect–Respond–Recover

7.1 Prevent and Detect

[78] Pankaj Nigam v. Union of India & Ors., W.P.(C) PIL, Delhi High Court (Division Bench: Chief Justice Devendra Kumar Upadhyaya and Justice Tejas Karia), notice issued 18 February 2026. Filed through Advocates Nishchaya Nigam (Managing Partner, Macrus Legal Law Offices) and C. Ankeeta Appanna.

[79] Allen & Overy Shearman Sterling LLP. (2025). Combatting payment account fraud: Singapore's Shared Responsibility Framework. A&O Shearman Insights. https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/combatting-payment-account-fraud-singapores-shared-responsibility-framework

[80] Financial Services and Markets Act 2023, c. 29, § 72 (UK). Royal Assent: 29 June 2023

In the payment infrastructure, the reporting and containment are integrated into the strategy of Brazil. The MED and the new dispute-button system allow the users to block funds on their banking applications with a certain period of time allocated on the investigation and resolution. The main operational problem of the quick disappearance of funds is solved not only by the multi-layer tracing feature of MED 2.0[81] that enables blocking of funds in the chain of fraud victims, but also by the initial victim. However, refunds using **MED** are often ineffective because scammer accounts are often emptied before blocks can be executed in 2023, and even successful MED refunds do not always cover the full value of the reported scam, just around 35 per cent of successful MED refunds.

The regime of the UK is concerned with the post-fraud reimbursal, which is based on the timeframes and cost sharing. The PSR will provide the data of monthly submissions of APP-fraud claims data which shall be published to make the PSPs have transparency and reputation to invest to prevent fraud. The provision of a live intervention tool: The power to suspend payment that is made by the suspect to up to four days of business by the Payment Services (Amendment) Regulations 2024 is an operating tool. The third party dispute-resolution is the Financial Ombudsman Service (FOS) which has the power to award compensation of up to 430,000 per complaint, which is an excellent accountability mechanism against PSPs that deny valid reimbursement claims.[82]

Singapore SRF implements a four-step claim procedure, which includes claim, investigation (2145 business days), outcome and recourse and external review body may be adopted as ***the Financial Industry Disputes Resolution Centre (FIDReC).*** The Protection from Scams Bill must bring in a new real-time intervention tool: Restriction Orders imposed by the police, which may freeze the banking operations of a potential victim until 30 days elapse, and which may be renewed up to five times, should respond to those who do not believe they have been a victim of scam.Institutional response metrics should not be limited to a number of raw complaints but it should include average times-to-freeze, percentage of money successfully recovered, timelines of in response, and repeat-victimisation rates, as well as The compilation and publication of Prevent-Detect-Respond-Recover framework suggests the obligatory confirmation-of-payee, risk-based step-up authentication, anti-fraud database operated by

[81] Banco Central do Brasil, Resolution BCB No. 1 of 12 August 2020 (Pix Regulation); Resolution No. 493 of 28 August 2025; Resolution No. 506 (September 2025); Resolution No. 507 (September 2025)

[82] Ministry of Home Affairs, Government of India. (2024). Indian Cyber Crime Coordination Centre (I4C). Established 2018; set up as Attached Office of MHA with effect from 1 July 2024. Operates the Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS) and Helpline 1930. As of 31 October 2025, financial amount of more than ₹7,130 crore saved in more than 23.02 lakh complaints. See also: Kumar, A. (2025). A critical study of the role and reform of the Indian Cyber Crime Coordination Centre. Journal of Neonatal Surgery (Multidisciplinary Issue), 14(7S). https://jneonatalsurg.com/index.php/jns/article/view/9955

NPCI, real-time SIM-swap, and standard UI/UX protection to prevent and identify UPI fraud. To recover and respond, it suggests gold-hour freeze measures, six-layer fund tracing based on Brazilian MED 2.0, and APP-fraud reimbursement regime, which assumes that reimbursement is not provided in case of gross negligence, the split expenses between sending and receiving PSPs and a five-business-day schedule. An ideal policy checklist will also mandate consumer-liability capped, jointly held databases, single complaint portals and availability of fraud statistics so that the markets is disciplined as well as the regulatory bodies are accountable.

Conclusion

8.1 Synthesis

The experience of UPI, Pix, and the UK Faster Payments system demonstrates that fast-payment rails, while transformative for financial inclusion and economic efficiency, structurally favour scam-driven APP fraud unless governance architectures evolve to rebalance responsibility across the ecosystem. The dominant fraud vector is not technical hacking but social engineering—exploiting UI confusion, fake customer-support impersonation, collect-request deceptions, and mule-account networks—in a settlement environment where near-instant irrevocability and the absence of chargeback mechanisms severely limit post-fraud remedies.

Comparative analysis reveals three distinct evolutionary stages in fast-payment fraud governance. Brazil's Pix has pioneered embedded dispute and refund mechanisms—the MED, MED 2.0, and the dispute button—integrating fraud containment within the payment infrastructure itself, though low realised recovery rates highlight the need for faster multi-layer blocking. The UK has led in aligning liability with APP-fraud realities through mandatory reimbursement, 50-50 cost-sharing between PSPs, a high "gross negligence" threshold for denying claims, and robust transparency requirements—creating powerful financial incentives for systemic fraud prevention. Singapore's SRF and Protection from Scams Bill add innovative elements: defined intermediary obligations across financial institutions and telecoms, a "waterfall" liability model, and police-issued Restriction Orders for real-time victim protection. India's UPI framework, by contrast, remains anchored in the "unauthorised transaction" paradigm of the RBI's 2017 circular, with evolving but fragmented judicial and quasi-judicial responses, and an institutional architecture under active judicial scrutiny for its coordination gaps and inadequate single-window redress.

8.2 Recommendations for Reform

- The main recommendation that the paper suggests to India is that the country should consider using a multifaceted Prevent-Detect-Respond-Recover model of governing UPI and fast-payment fraud, which incorporates the following reforms:
- Legal transparency on APP-fraud liability: The RBI ought to give a particular circular, or the legislature ought to modify the PSS Act, to cover the "authorised but caused transactions to the effect of a presumption of reimbursement with an exception of gross-negligence to the burden of the PSP, based on the UK in the section of 72 of the Financial Services and Markets Act 2023.
- Confirmation-of-payee and risk-based friction, though, is not mandatory: NPCI, under the guidance of RBI, must enforce real-time payee-name validation and step-up authentication, which is normally standardised in high-risk transactions using UPI. Centralised fraud-intelligence infrastructure: anti-fraud database and fund-tracing multi-layer-capability The name of the game is a shared, privacy-consistent anti-fraud data pool and the ability to trace funds, following the Pix MED 2.0 concept and its anti-fraud data bank, should be operationalised in the infrastructure of the NPCI with compulsory PSP membership. Built-in reporting: A single, in-app complaint system connected to banks, NPCI, telecoms and law enforcement - with time-limited freeze plans in place - must replace the existing multi-window structure, which is desired in the proposed PIL of the Delhi High Court.
- TELECOM-layer responsibility The framework must establish clear SIM-swap verification and anti-spoofing responsibilities on the UPI authentication chain of telecom operators, based on Singapore SRF model of responsible telecoms.
- Transparency and market discipline: The RBI and NPCI are to enforce and make public regular APP-fraud and reimbursement data of all large PSPs so that the regulators can benchmark and consumers make a choice.
- Capacity building: The scheme would empower the quality and speed of the resolution of disputes by having specialised cyber-fraud adjudication benches in consumer fora and in the RBI Ombudsman scheme, which have technical expertise and access to digital evidence.

Further studies are needed to strengthen the empirical character of this study by the availability of granular fraud-incident data, PSP-levels controls, and victim accounts, such as the varies effect of UPI scams on vulnerable users, women, and small merchants. The interaction of instant-payment fraud and

the changing data-protection regimes, open-banking programs, and various cross-border payment solutions should also be studied through cross-jurisdictional studies to determine whether their proposed models of liability and governance can be extrapolated to international rails.