The Dialogue®
INFORM ENGAGE IDEATE

IN COLLABORATION WITH

SUPPORTED BY

TOWARDS SAFER AND SMARTER

DIGITAL PAYMENT SYSTEMS

A POLICY REPORT

MAY 2026

TRUST | COORDINATION | SPEED | INCLUSION | GROWTH

ONE ECOSYSTEM. ONE RESPONSE.

A SECURE DIGITAL FUTURE FOR EVERY INDIAN.

Towards Safer and Smarter Digital Payment Systems

Author: Raunaq Sharma

Contributors: Ranjeet Rane, Aastha Tiwari, Soham Jagtap and Kriti Singh

Copyeditor: Akriti Jayant

Thematic Designer: Shivam Kulshrestha

About The Dialogue: The Dialogue is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

About The Centre for Information Communication Technology and Law, MNLU Mumbai: The Centre for Information Communication Technology and Law (CICTL) is committed to advancing research and dialogue at the intersection of technology and law. It explores emerging opportunities and challenges in the information society, develops legal and policy solutions, and brings together experts from technical and legal domains. Through research, collaborations, and advisory services, the Centre contributes to informed techno-legal discourse and supports effective governance in the digital age.

About Maharashtra National Law University, Mumbai: Maharashtra National Law University, Mumbai (MNLU Mumbai), established under the Maharashtra National Law University Act, 2014, is a premier institution for advanced legal education and research in India. Since commencing academic operations in August 2015, the University has focused on disseminating legal knowledge, building advocacy and reform-oriented skills, and promoting research that contributes to societal development. In a short span, MNLU Mumbai has made significant strides in strengthening legal scholarship and shaping future-ready legal professionals.

For more information
Visit: thedialogue.org.in | mnlumumbai.edu.in

Suggested Citation
Sharma, R. (May, 2026) Policy Report: Towards Safer and Smarter Digital Payment Systems. The Dialogue, CICTL and MNLU.

Catalogue No.
TD/DE/PR/0526/05

Publication Date
May 9, 2026

Table of Contents

List of Abbreviations

Abbreviation	Full Form
AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
APK	Android Package Kit
BNS	Bharatiya Nyaya Sanhita
BNSS	Bharatiya Nagarik Suraksha Sanhita
BSA	Bharatiya Sakshya Adhiniyam
CBI	Central Bureau of Investigation
CEIR	Central Equipment Identity Register
CERT-In	Indian Computer Emergency Response Team
CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
CIOR	Calling Line Identity-based International Incoming Spoofed Calls Prevention System
DIP	Digital Intelligence Platform
DPIP	Digital Payments Intelligence Platform
DPDP Act	Digital Personal Data Protection Act, 2023
DoT	Department of Telecommunications
FCA	Financial Conduct Authority
FIR	First Information Report
FIU-IND	Financial Intelligence Unit–India
FREE-AI	Framework for Responsible and Ethical Enablement of AI
FRI	Financial Fraud Risk Indicator
FSB	Financial Stability Board
I4C	Indian Cyber Crime Coordination Centre
IDPIC	Indian Digital Payments Intelligence Company
IMEI	International Mobile Equipment Identity
IMPS	Immediate Payment Service
IVR	Interactive Voice Response

JAM	Jan Dhan–Aadhaar–Mobile
KRI	Key Risk Indicators
KYC	Know Your Customer
MHA	Ministry of Home Affairs
MNRL	Mobile Number Revocation List
MoU	Memorandum of Understanding
NBFC	Non-Banking Financial Company
NCB	Narcotics Control Bureau
NCRP	National Cybercrime Reporting Portal
NEFT	National Electronic Funds Transfer
NPCI	National Payments Corporation of India
OTP	One-Time Password
PSD2	Revised Payment Services Directive
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
SIM	Subscriber Identity Module
SOP	Standard Operating Procedure
TRAI	Telecom Regulatory Authority of India
UPI	Unified Payments Interface
VDA	Virtual Digital Asset
VoIP	Voice over Internet Protocol

Executive Summary

India has built one of the largest digital payment systems in the world. In the financial year 2024-2025, the country processed about 28,834 crore digital transactions, with the Unified Payments Interface (UPI) alone accounting for more than four-fifths of this flow. However, the same architecture that brought a billion users into formal finance has also expanded the attack surface. Reported losses from cyber fraud reached around ₹ 22,495 crore in 2025, compared to ₹ 22,845 crore in 2024 and ₹ 7,465 crore in 2023. While total losses have remained relatively stable, the number of cases continues to rise, indicating that the attack surface is expanding even as enforcement begins to contain individual losses.

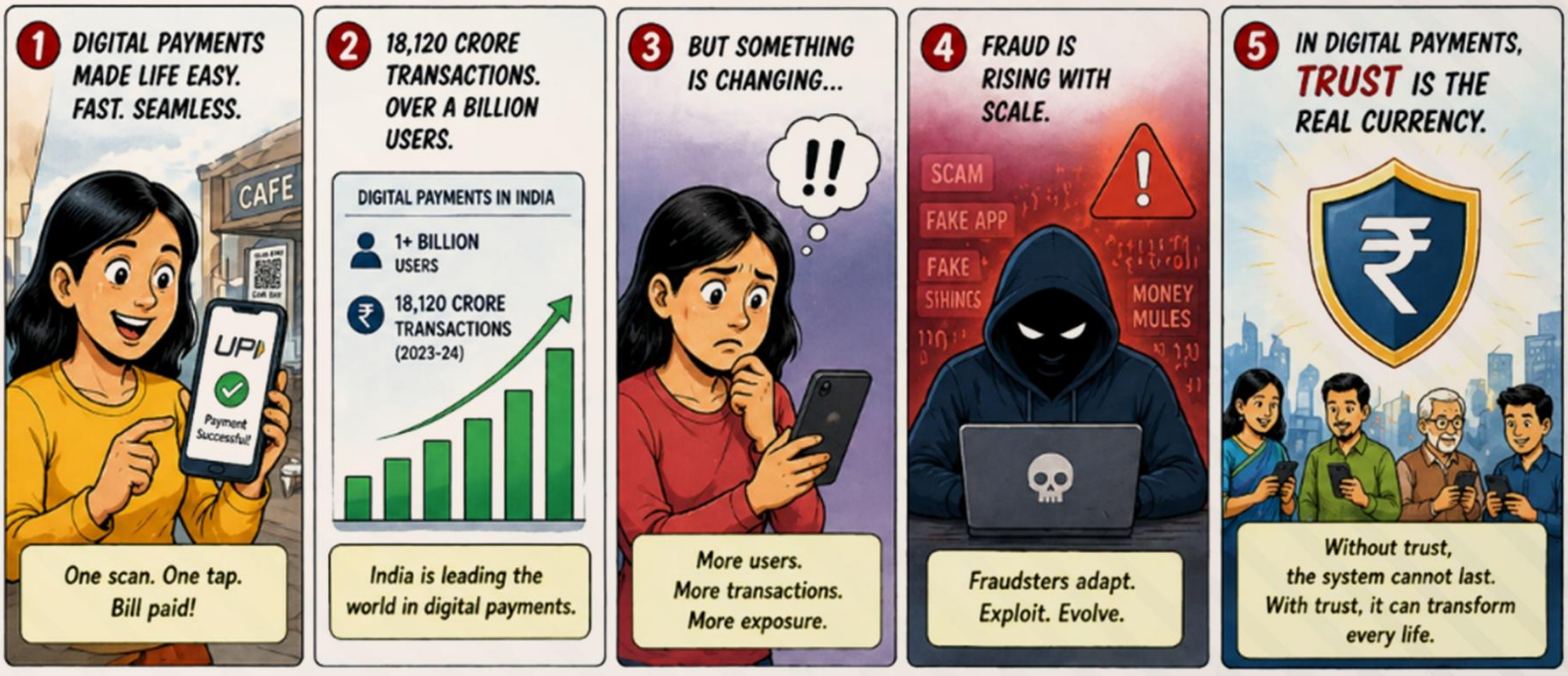
The character of fraud in India has evolved significantly. While traditional hacking and unauthorised access remain relevant, a growing share of high-value scams today, including digital arrest, investment and trading frauds, and mule account-driven laundering, rely less on technical compromise and more on exploiting human vulnerabilities. These scams use psychological manipulation, artificial time pressure, and the strategic misuse of institutional symbols such as courts, regulators, and law enforcement to coerce victims into authorising payment. Investment scams alone accounted for a large share of losses in 2025. The fraud economy now resembles a structured cross-border industry, with a significant portion of operations linked to scam compounds in Southeast Asia and funds routed through layered mule accounts within India.

In response, the institutional framework has expanded but remains fragmented. The 1930 helpline, the National Cybercrime Reporting Portal (NCRP), the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), the Financial Fraud Risk Indicator (FRI), the Suspect Registry, MuleHunter.AI, and the Digital Payments Intelligence Platform (DPIP) together form a substantial response stack. However, these systems do not yet operate as a unified national layer. Intelligence generated at one point often fails to translate into timely action at another. Most banks continue to rely on rule-based monitoring, and only 21% of Reserve Bank of India (RBI)-regulated entities use Artificial Intelligence (AI) in any form. As a result, while prevention metrics improve, recovery rates for victims remain limited.

This report argues that the next stage of reform should focus on consolidation. The recommendations cluster around four areas. First, the Government of India should build a national fraud intelligence and response layer that brings banks, Non-Banking Financial Companies (NBFCs), UPI participants, payment aggregators, wallets, telecom actors, and law enforcement into a common operational chain, with shared case identities and binding response timelines. Second, Parliament and the RBI should establish an explicit legal basis for cross-institutional fraud data sharing, protective restraint, and victim compensation, building on the RBI's draft compensation scheme of March 2026. Third, the National Payments Corporation of India (NPCI) and payment system providers should redesign transaction flows to embed verification, cooling-off periods, trusted contact alerts, and conditional holds for flagged transfers, drawing on the RBI *Authentication Mechanisms for Digital Payment Transactions Directions* issued in September 2025. Fourth, the RBI and NPCI should embed accessibility and inclusive design in fraud safeguards so that protections reach senior citizens, rural users, persons with disabilities, and non-English speakers, including by extending Bhashini integration to fraud warning screens.

Recent policy direction, including the RBI discussion paper on safeguards, the March 2026 compensation scheme, and Payments Vision 2028, is broadly aligned with this approach. The priority now is to bring the existing components within a single operational and governance framework, supported by enforceable timelines and outcome-based measurement.

1. Introduction



India has redesigned the foundations of its financial system in a way few nations have achieved. The national digital stack, built on the Jan Dhan-Aadhaar-Mobile (JAM) trinity and the UPI, has expanded formal financial access to more than a billion people. In the financial year 2024-2025, digital payment systems processed about 18,120 crore transactions, with UPI accounting for more than four-fifths of this flow.[1] This shift from cash to digital has delivered three core benefits: improved inclusion, reduced friction in the economy, and stronger participation in formal markets.

However, this transformation has also created new vulnerabilities. As participation in the digital economy expands, criminals have shifted their focus from large institutions to individual users. Today, cyber fraud operates primarily through deception, relying on psychological manipulation rather than technical sophistication. In 2025, reported losses from cyber fraud in India reached around ₹22,495 crore. At the first glance, this reflects a slight decrease from ₹22,845 crore in 2024. However, a comparison between 2023 and 2024 reveals a steep increase of 206%.[2]

This growing threat undermines confidence in the system. For instance, a first-time digital user who falls victim to a fake investment pitch or a “digital arrest” scam often loses trust in digital services and reverts to cash. Trust, therefore, becomes the real currency of the digital economy. Without it, the gains made in financial inclusion begin to erode.

The report analyses the evolving cyber fraud landscape in India, maps the institutional and regulatory response, and identifies the structural gaps that continue to undermine prevention, detection, and redress.

The report offers policy recommendations that focus on the following areas:

- Build a national fraud intelligence and response layer that brings together banks, telecom operators, payment platforms, and law enforcement into a unified operational chain, with shared case identities and binding response standards.
- Reform legal and regulatory frameworks to establish a clear basis for cross-institutional fraud data sharing.
- Redesign transaction flows to embed verification, delay, and human intervention mechanisms that protect users during high-risk transfers.
- Embed accessibility and inclusive design in fraud safeguards to ensure that protections reach senior citizens, rural users, persons with disabilities, and non-English speakers.

1.1 What does trust mean in the context of digital payments

Trust is crucial in fintech platforms, as users entrust digital systems with their financial transactions and sensitive personal data. Discussions on digital payments often reduce trust to security features, but for users, its meaning is far broader. It is the assurance that a payment will reach its intended destination, that warnings are clear and understandable, that risks surface before irreversible harm occurs, and that

[1] Ministry of Finance. (2025, March 11). RBI, NPCI launch awareness campaigns and AI-based solutions to prevent financial cybercrimes (Press Release ID 2110405). Press Information Bureau. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405

[2] Tewari, S. (2026, February 21). Cybercrime saw 24% spike in 2025. Indians lost Rs 22,495 crore, mainly in investment scams. ThePrint. https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/

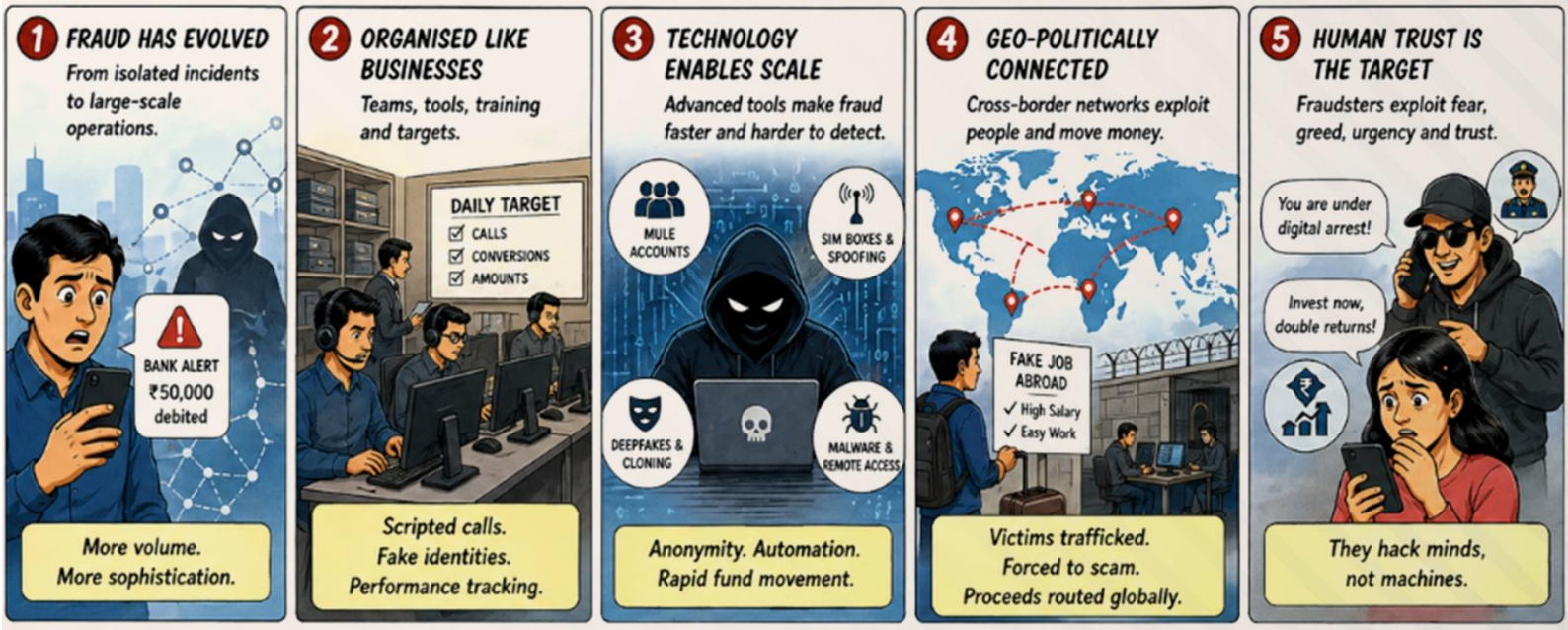
the system responds quickly if something goes wrong. In other words, trust is a property of the overall architecture that shapes user confidence and determines how effectively institutions resolve problems.

In emerging digital ecosystems, users perceive trust through institutional credibility and consistent communication. However, this very trust can become a vector for exploitation in environments marked by informational asymmetry and low digital literacy. Ideally, access to digital finance would align with users' ability to use it securely. In India, however, many newly banked individuals, particularly in rural areas and among older populations, lack the digital literacy needed to protect themselves. This gap has contributed to a sharp rise in fraud, with the Indian Computer Emergency Response Team (CERT-In) reporting a 58% increase in user-targeted fraud between 2022 and 2024, largely driven by phishing attacks. As a result, a gap has emerged between access and awareness, giving rise to what scholars term the "digital vulnerability paradox," where technologies designed to promote inclusion also increase users' exposure to exploitation.

This issue is particularly important today because modern fraud often works by compressing time and attention. It pushes users into rapid decisions and isolates them from reliable verification channels, exploiting gaps between institutions that are individually responsible but collectively uncoordinated. If trust depends on each user behaving like an expert, it will fail at national scale.

2.

The Evolving Cyber Fraud Landscape in India



India is experiencing cyber fraud at a scale that goes well beyond isolated incidents. As highlighted earlier, the magnitude of financial losses now reflects a mature criminal economy. The figures from 2025 (₹ 22,495 crore) are nearly three times the ₹ 7,465 crores reported in 2023 and close to ten times the ₹ 2,306 crore recorded in 2022. This trend reflects both the expanding reach of fraud syndicates and improved reporting through newer cybercrime platforms. The volume of reported financial fraud cases has also increased in parallel, rising from about 24.4 lakh cases in 2023 to 28.15 lakh cases in 2025, far exceeding earlier levels, including roughly 10 lakh cases in 2022.[3] These trends underscore that fraud persists at an epidemic scale.

While enforcement interventions have improved outcomes at the margin, recovery remains limited, and the overall economic damage is substantial. In 2024, for instance, out of a total loss of ₹ 22,845 crore, interventions by law enforcement agencies resulted in recoveries of ₹ 5,489 crore,[4] only a fraction of the total amount lost.

Table 1: Digital Payment Transactions and Cyber Fraud in India (FY 2019-20 to FY 2025-26)

Financial Year	Volume of Digital Payments (crore)	Cyber Fraud Losses (₹ crore)	Fraud Complaints (lakh)[5]	CY Ref.
FY 2021-22	7,197	551.65	4.52	2021
FY 2022-23	11,393	2,290	10.29	2022
FY 2023-24	16,443	7,463	15.96	2023
FY 2024-25	28,834	22,846	22.68	2024
FY 2025-26	28,031	22,495	28.15	2025

Note: Payment data follows the Indian financial year (April to March). Cyber fraud losses and complaint figures are reported by calendar year. Each financial year row is mapped to the calendar year in which the majority of its months fall (e.g., FY 2024-25 maps to CY 2024, since ten of its twelve months fall within that calendar year). The last column indicates the calendar year reference used for the fraud data. Payment data is sourced from the Department of Financial Services, the National Payments Corporation of India, and the Reserve Bank of India. Fraud data is compiled from Indian Cyber Crime Coordination Centre reports and Ministry of Home Affairs disclosures to Parliament.

2.1 The Anatomy of Modern Fraud as Psychological Crime

As discussed above, modern cyber fraud in India extends beyond technical sophistication and relies primarily on advanced psychological manipulation. The tools used today are scripts and emotional triggers rather than malware or brute-force intrusions. A victim who transfers life savings under a fake "digital arrest" or invests money in a fabricated trading platform is not hacked in the traditional sense; instead, they are manipulated into acting against their own interests through sustained psychological

[3] TOI Business Desk. (2025b, July 22). India's cyber fraud epidemic: Rs 22,845 crore lost in 2024; 206% jump from previous year, says government. The Times of India. https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms
[4] TOI Business Desk. (2025b, July 22). India's cyber fraud epidemic: Rs 22,845 crore lost in 2024; 206% jump from previous year, says government. The Times of India. https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms
[5] Jadhav, V. (2025, December 6). Complaints rose fivefold since 2021, and digital payment and 'digital arrest' scams surged. IndiaSpend. https://www.indiaspend.com/data-viz/dataviz-how-indias-cyber-crime-incidence-is-rising-972933

pressure. Understanding how and why this occurs is essential to designing interventions that move beyond awareness campaigns and address the cognitive and emotional architecture of victimisation.

Two emotions underpin most large-scale scam scripts in India today: fear and greed. Fear-driven scams, including digital arrest and impersonation frauds, compress time and induce a threat state in which victims lose the ability to think clearly. Greed-based scams, such as investment frauds and task-based job schemes, expand time and build trust gradually until the victim becomes so financially and emotionally committed that withdrawal feels more painful than continued compliance. The former exploits loss aversion, while latter exploits aspiration. Both, however, rely on the same underlying principle: human cognition is not designed to function effectively under such conditions.

The behavioral economist Daniel Kahneman described two systems of thinking that govern human decision making. System 1 is fast and heuristic-driven while System 2 is slow and analytical. Under normal circumstances, System 2 moderates the impulses of System 1. However, in situations of fear and urgency, System 2 is suppressed. Scam scripts are deliberately designed to recreate these conditions. As a result, a victim who is told they face imminent arrest may not pause to verify the claim, because their fear response overrides their capacity for reflective judgment.

Robert Cialdini's principles of persuasion complement this analysis.[6] His work identifies six mechanisms through which people are influenced: authority, scarcity, social proof, reciprocity, commitment and consistency, and liking. Each of these operates across major scam typologies in India. Digital arrest scams exploit authority and scarcity of time in their most direct forms, a fake police officer establishes authority, while the threat of imminent arrest creates urgency. Investment scams rely on social proof through fabricated group chats and testimonials, liking through sustained rapport-building, and commitment and consistency by encouraging small investments that escalate over time.

Another interesting concept is “dark creativity,” developed by Hansika Kapoor and James Kaufman, which describes the application of original thinking toward harmful ends.[7] Kapoor's AMORAL framework maps the antecedents, mechanisms, and aftereffects of creative harm, and her empirical work examines how dark creativity manifests across cultures, including in India's financial fraud landscape.[8] The scripts used in digital arrest and “pig butchering” scams continuously evolve in response to awareness campaigns and enforcement actions. Over time, each incident contributes to an adaptive ecosystem in which criminal networks refine their persuasion strategies based on what has proven effective.

Shame and stigma function as a secondary enforcement mechanism that keeps victims silent even after the fraud has occurred. The dynamic is particularly pronounced in India, where cultural expectations around financial prudence and family reputation can discourage victims from disclosing incidents or filing formal complaints. Scammers actively exploit this. Digital arrest scripts often instruct victims to maintain strict secrecy, while investment fraud operators build emotional rapport that makes victims feel complicit in their own loss. In this sense, shame is deliberately engineered into scam design as a barrier to reporting and intervention.

Cultural context further amplifies these vulnerabilities. India scores 77 on Geert Hofstede's Power Distance Index, placing it among the highest power-distance societies globally.[9] This reflects a deeply

---

[6] Robert B. Cialdini, Influence: The Psychology of Persuasion (HarperCollins, 1984; revised 2021). The six principles are authority, scarcity, social proof, reciprocity, commitment and consistency, and liking. A seventh, unity, was added in Pre-Suasion (2016)

[7] Hansika Kapoor and James C. Kaufman, The Evil Within: The AMORAL Model of Dark Creativity, Theory and Psychology, 2022. The AMORAL framework describes Antecedents, Mechanisms, Operants, Realisation, Aftereffects, and Legacy of creative harm

[8] Hansika Kapoor et al., Shining a Light on Dark Creativity, Creativity Research Journal, 37(2), 2025, pp. 236–241.

[9] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, Cultures and Organizations: Software of the Mind, 3rd ed., McGraw-Hill, 2010. India scores 77 on Hofstede’s Power Distance Index, against a global average of roughly 56.5

embedded deference to perceived authority. A 2025 analysis by the Lowy Institute linked this directly to susceptibility to digital arrest scams, noting that 79% of Indians report trust in government institutions, compared to 47% in Australia and 41% in the United States.[10] Scammers exploit what psychologists describe as "destructive obedience," where individuals comply with instructions because they believe the authority issuing them is legitimate and that non-compliance will lead to serious consequences.

These psychological and cultural factors operate alongside technological enablers, including spoofed caller IDs, deepfake audio and video, mule account networks etc. Fraud, therefore, emerges from the intersection of human vulnerability, engineered scam design, and enabling infrastructure.

2.1.1 Digital arrest scams, impersonation and fear tactics

Digital arrest scams are distinctive in how they immobilise victims through a simulated interface of state control. They operate as a cyber extortion, where victims are led to believe they are in official custody without any physical presence of law enforcement.

These scams typically begin with unsolicited outreach, such as an IVR call or text message impersonating a trusted government agency. Common impersonations include officials from the Telecom Regulatory Authority of India (TRAI), the Central Bureau of Investigation (CBI), the Narcotics Control Bureau (NCB), or Customs and Excise. The initial hook is often an artificial crisis: victims are told that a parcel addressed to them contains illegal substances and fake passports, that their Aadhaar has been used to open bank accounts linked to money laundering, or that their mobile number will be disconnected for alleged involvement in unlawful activities.

Once the victim takes the threat seriously, the scam escalates to a video call, often conducted through popular messaging platforms. The visual staging is carefully constructed: perpetrators use police-style uniforms, backdrops resembling stations or courtrooms, national symbols, and forged identification. Victims are told they are under "digital custody" or "virtual arrest." They are instructed to keep their camera on continuously, isolate themselves from family or legal counsel, and maintain strict secrecy. These instructions are often reinforced by threats invoking laws such as the Official Secrets Act or the risk of imminent non-bailable arrest. [11]

Psychologically, these scams draw on mechanisms such as dark creativity and power distance. In India, cultural conditioning often produces high deference to perceived authority. Scammers exploit this by triggering what psychologists describe as an "amygdala hijack," an intense fear response that suppresses rational, deliberative thinking and compels immediate compliance.[12]

The financial extraction stage is framed as a form of "verification," where victims are told to transfer their funds to a so-called supervision account or verification wallet to prove that the money is not linked to criminal activity. To reinforce credibility, scammers often issue fabricated documents, such as an "Innocence Verification Certificate." Once the transfer is completed, communication abruptly ends and the impersonated officials disappear.

[10] Lowy Institute, India's Digital Arrest Scams, The Interpreter, 2025. The analysis notes that 79 per cent of Indians trust government, compared to 47 per cent in Australia and 41 per cent in the United States, citing the 2025 Edelman Trust Barometer

[11] Niti Aayog. Digital Arrest: The Modern-Day Cyber Scam. https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf

[12] Kapoor, H., PhD. (2025, April 1). New-age financial scams are becoming more original and evil. Psychology Today. https://www.psychologytoday.com/us/blog/dark-creativity/202504/the-ingenious-harm-caused-by-digital-arrests-in-india?utm

2.1.2 Investment and trading frauds: trust building followed by greed exploitation

While digital arrest scams rely on fear, investment scams exploit the sunk cost fallacy and the human need for connection. The most prominent typology is "pig butchering," derived from the Chinese term *Sha Zhu Pan*, which reflects the prolonged process of building up a victim before extracting money.

The first phase is grooming, often described as "fattening." Unlike the rapid escalation seen in digital arrest scams, this process unfolds gradually. It typically begins with a seemingly harmless interaction, such as a wrong-number message, a connection on a dating app, or engagement through a job portal. The scammer constructs a credible, often aspirational persona, and spends weeks or even months building rapport, deliberately avoiding any early requests for money. The goal is to create trust and establish emotional dependency.

The second phase is the investment hook. The conversation gradually shifts to wealth and financial success. The scammer introduces a guaranteed platform, often presented as cryptocurrency investing. The victim is guided to a fake trading app controlled by the syndicate and encouraged to start small. Early on, the victim is allowed to withdraw profits, creating social proof and reinforcing the belief that the platform is legitimate.

The third phase is extraction. Once convinced, victims are pressured to invest their entire savings, take loans, or liquidate assets. When they attempt to withdraw a large sum, the platform freezes. The scammer demands payments framed as taxes, handling fees, or security deposits to unfreeze the account. Victims then pay additional amounts in an effort to recover what they have already invested, a classic sunk cost trap.[13][14]

2.1.3 Mule account recruitment, gamified fraud networks via Messaging Platforms

Many cyber frauds rely on an infrastructure of money mules, meaning bank accounts used to move illicit funds. Criminal syndicates have turned mule recruitment into a structured, and sometimes gamified operation. The psychological play targets individuals who are desperate or unaware, lured by the promise of quick money. Recruiters cast a wide net, and messages advertising easy passive income or part-time jobs attract students, unemployed youth, and others in need of cash. Reports suggest that recruitment frequently takes place through groups on popular messaging platforms.

Fraudsters circulate malicious Android apps or links within these groups, often disguised as income generators, investment tools, or simple wallets. Once installed, these apps request extensive permissions such as SMS access and device control. These permissions allow scammers to hijack accounts, approve transactions, and capture One-Time Passwords (OTPs) in the background. Recruits are promised

[13] Bahl, A. (2025, November 27). Former IT firm owner loses over Rs 2 crore in stock market investment scam. *The Times of India*. https://timesofindia.indiatimes.com/city/noida/former-it-firm-owner-loses-over-rs-2-crore-in-stock-market-investment-scam/articleshow/125598923.cms

[14] Deshkar, A. (2025, May 2). He lost Rs 90 lakh after joining a WhatsApp group: Investment scams are raging, here's how to stay safe. *The Indian Express*. https://indianexpress.com/article/technology/tech-news-technology/investments-scams-how-to-spot-protect-safe-side-9796966/

commissions of about 2% to 3% on large transaction volumes as account agents. They may initially receive a small reward, reinforcing the perception of legitimacy.

While this process may appear to be carried out by a single individual, organised networks typically manage these mules. Local agents, coordinated through online messaging groups, approach individuals in villages, colleges, or low-income areas and offer fixed payouts for access to bank accounts. For instance, a recruiter might pay ₹ 10,000 to ₹ 20,000 for a basic savings account, and significantly more for corporate accounts with higher transfer limits. Reports have cited amounts as high as ₹ 4 to ₹ 5 crores upfront for access to accounts with limits of ₹ 100 crore. Once enrolled, the mule's direct role may be minimal. The syndicate often takes control of debit cards, cheque books, and linked Subscriber Identity Module (SIM) cards. The account then becomes a conduit for laundering victim funds, with money rapidly routed through multiple mule accounts across states and sometimes across borders before authorities can intervene.

These networks can resemble pyramidal structures, where handlers in major hubs manage agents below them. In some instances, performance is gamified, with top earners ranked and rewarded. Certain mule account holders have reportedly earned commissions as high as ₹ 1.2 crore for quickly transferring stolen funds. However, these cases are not uniform. Some recruits may not fully understand the illegality of their actions and are told they are consultants or payment processors, while others knowingly participate for a share of the proceeds. The promise of life-changing income serves as a powerful incentive, ensuring a steady supply of mule accounts, particularly among economically vulnerable groups.

Table 2: Additional common scam typologies in India's digital payments ecosystem

Scam type	How it typically works	Common user touchpoint
Refund and reversal plus collect request deception	The victim is told they will receive money, but is pushed to approve a collect request or payment prompt and enter a UPI PIN, which results in a debit. NPCI has moved to discontinue person-to-person collect requests from October 1, 2025.	UPI collect request, refund messages, seller-to-buyer interactions
QR code social engineering	The victim is told to scan a QR code to receive money, but the scan initiates an outgoing payment flow once confirmed with a PIN.	Marketplace sales, refunds, informal transfers
QR code tampering	A legitimate merchant QR is replaced or overlaid so that payments are routed to a fraudster's account.	Shops, printed QR stands, public payment points
Fake customer care and search manipulation	The victim searches for support numbers, reaches an impostor helpline, and is then coached into sharing OTPs, approving payment prompts, or installing apps.	Search results, sponsored links, social media pages

Remote access and screen sharing fraud	The victim installs a remote access or screen-sharing tool for assistance, The attacker observes OTPs and approvals and may guide or control transactions.	Customer support impersonation, refund scripts
Malicious Android Package Kit (APK) and phishing link delivery	The victim clicks a link and installs a fake app or opens a phishing page, often framed as Know Your Customer (KYC) updates, service disconnection, challans, or courier redelivery. Permissions or credentials are then captured.	Text messaging platforms, SMS, email, fake websites
SIM swap and account takeover	The victim's phone number is hijacked, allowing interception of OTPs and account reset requests, leading to takeover of bank or UPI access.	Telecom channels and banking reset processes
Fake payment confirmation	The fraudster shows an edited screenshot or fake success message and leaves before the recipient verifies the transaction in their own app.	Offline sales, delivery payments, small merchants
Mandate and AutoPay prompt abuse	The victim is persuaded to approve a mandate or recurring authorisation, sometimes framed as a verification step, leading to repeated debits.	UPI prompts and mandate requests
Advance fee and booking scams	A fake booking or service platform extracts an upfront payment and then disappears or continues to demand additional fees.	Travel, bookings tickets, pilgrimages, service platforms
Impersonation scripts in mass fraud reporting	Scam prompts often mirror standardised categories used in the Department of Telecommunications (DoT) Chakshu, including KYC updates and impersonation of officials.	Calls, SMS, text messaging platforms, spoofed sender IDs

2.2 The Technical Infrastructure

Cyber fraud at scale depends on systems that make three things easy. First, reaching victims at scale while hiding the caller's true location and identity. Second, moving stolen funds quickly across multiple accounts before banks or law enforcement can freeze them. Third, shifting value out of the regulated banking system, often across borders, in forms that can be stored and transferred with limited friction.

Recent enforcement efforts show that fraud networks treat each of these as an engineering problem, building redundancies across layers to remain operational even when one link fails.

2.2.1 The Mule Ecosystem

Mule accounts remain the basic financial unit of cyber fraud because they convert a victim's single transfer into a complex, hard-to-trace trail. Many accounts are provided through an account-renting model, where individuals knowingly hand over access to their banking instruments and identifiers, often including account kits such as cards, cheque books, and linked SIMs, in exchange for commissions. Gujarat's Operation Mule Hunt is a good example of how enforcement now treats mule account creation as an organised market.

Once money enters this layer, the priority is speed. Funds are split, forwarded, and re-forwarded through multiple accounts so that investigators are forced into a multi-bank and multi-branch coordination exercise. This is why the first hours matter. Government systems that focus on this early window include the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) for rapid reporting and blocking, and the Cyber Fraud Mitigation Centre model that brings banks, payment intermediaries, telecom providers, and law enforcement together for immediate action.

The same logic is visible in how the state is turning mule accounts into a shared intelligence signal across institutions. A Suspect Registry was launched in September 2024 in collaboration with banks and financial institutions, with official disclosures noting large volumes of suspect identifiers and layer 1 mule accounts shared across entities, and declined transactions running into thousands of crores. These mechanisms aim to stop the laundering chain before it becomes a long trail of small transfers that are expensive to unwind.

Fraud networks also use mule accounts to build payment collection infrastructure that appears legitimate. The Ministry of Home Affairs (MHA), through the Indian Cyber Crime Coordination Centre (I4C), has warned about illegal payment gateways created using mule or rented accounts, describing them as a "money laundering as a service" layer used by transnational cybercriminal groups. This marks an important shift, as mule accounts are now used to create stable collection rails that can be rotated quickly when flagged, beyond simple laundering. A July 2025 investigation by the cybersecurity firm CloudSEK documented Chinese cyber syndicates laundering over ₹ 5,000 crore annually through such illegal payment gateways operating in India.[15] The modus operandi involves recruiting Indian citizens as money mules via popular text messaging applications, collecting bank credentials and debit cards, and creating parallel payment processing infrastructure that sits entirely outside RBI regulation. Named illegal gateways identified in the investigation include PeacePay, RTX Pay, PoccoPay, and RPPay, all operated by foreign nationals.[16] One application analysed by CloudSEK showed $20 million laundered through 398,675 transactions involving 34,299 mule accounts.[17] I4C's October 2024 alert noted that approximately 50% of cybercrime complaints in India link back to entities in China, with Cambodia and Myanmar as other major source countries.[18]

---

[15] CloudSEK. (2025, July). Uncovering Chinese dark web syndicates and money mule pipeline to Indian banks [White paper]. https://www.cloudsek.com/whitepapers-reports/uncovering-chinese-dark-web-syndicates-and-money-mule-pipeline-to-indian-banks

[16] Press Information Bureau. (2024, October 28). Indian Cybercrime Coordination Centre (I4C), MHA issues alert against illegal payment gateways created using mule bank accounts by transnational organized cybercriminals facilitating money laundering as a service. Government of India. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2069000

[17] Uddin, D. (2025, July 15). Chinese groups launder $580M in India using fake apps and mule accounts. Hackread. https://hackread.com/chinese-groups-launder-india-fake-apps-mule-accounts/

[18] China, pockets of Cambodia and Myanmar are epicentre of cybercrime: I4C chief. (2024, January 3). The Hindu. https://www.thehindu.com/news/national/china-pockets-of-cambodia-and-myanmar-are-epicentre-of-cybercrime-i4c-chief/article67703371.ece

2.2.2 The Telecom Nexus

Fraud at a national scale requires industrial telecommunications capacity. SIM boxes, also described as SIM gateways, are one of the most direct ways to industrialise outreach. They allow hundreds of SIMs to be run in parallel so that calls and messages can be placed at scale, and numbers can be rotated quickly when victims complain or operators block them. A recurring pattern in Indian law enforcement investigations is the use of such setups to make overseas activity appear domestic. Police and telecom-led operations have documented SIM box rackets that convert international Voice over Internet Protocol (VoIP) calls into local calls, which reduces suspicion for the recipient and complicates attribution in the early stages of investigation.

Spoofing complements SIM box infrastructure by manipulating caller identity so that the number displayed to the victim appears to be a trusted government or institutional number. This is especially relevant to impersonation-driven scams, including digital arrest style scripts, where immediate credibility is critical before the target can verify the claim.

Multiple SIM box seizures in 2025 illustrate the scale of this infrastructure. In Andhra Pradesh, a December 2025 operation uncovered 14 SIM box devices, seized over 1,500 illegal SIM cards, and arrested 20 individuals in a network linked to losses exceeding ₹ 20 crore. Tamil Nadu's Cybercrime Wing arrested six suspects in August 2025, including a bank relationship manager and a telecom sales agent, and seized 14 high-capacity SIM box devices linked to Chinese handlers. Follow-up raids in November 2025 across Delhi, Bihar, and Maharashtra yielded 24 additional SIM boxes.[19][20]

2.2.3 Deepfake-Enabled Fraud

Deepfake technology has reached a level of accessibility and quality that makes it operationally significant for financial fraud. The threat manifests across multiple vectors. Real-time deepfakes using tools such as DeepFaceLive and Magicam can bypass video KYC calls, of which over 11 lakh are conducted daily in India.

To illustrate how far these deepfake techniques have evolved, in November 2024, a deepfake video impersonating the RBI Governor circulated widely on social media, with many unable to assess its authenticity.[21] These deepfake techniques enable the creation of synthetic identities, which can be used to open mule accounts without requiring human account holders.

Voice cloning has also advanced rapidly. Current AI models require only 3 to 10 seconds of audio to generate convincing voice replicas. Several such incidents related to voice cloning have been reported by cybercrime units across states over the past two years.[22] [23]

---

[19] Massive international SIM box technology cyber fraud busted in Andhra Pradesh. (2025, December 26). NDTV. https://www.ndtv.com/andhra-pradesh-news/massive-international-sim-box-technology-cyber-fraud-busted-in-andhra-pradesh-9984336

[20] Tamil Nadu cybercrime police bust SIM box network. (2025, October 6). The Hindu. https://www.thehindu.com/news/national/tamil-nadu/tamil-nadu-cybercrime-police-bust-sim-box-network/article70130468.ece

[21] CBI conducts searches at six locations & arrested two accused persons in connection with SIM Box-based cyber-enabled fraud operation. (2026, March 27). NewsOnAir. https://www.newsonair.gov.in/cbi-conducts-searches-at-six-locations-arrested-two-accused-persons-in-connection-with-sim-box-based-cyber-enabled-fraud-operation/

[22] Scamsters use AI to clone cousin's voice, dupe Indore teacher of Rs 1 lakh. (2026, January 10). NDTV. https://www.ndtv.com/india-news/scamsters-use-ai-to-clone-cousins-voice-dupe-indore-teacher-of-rs-1-lakh-10604289

[23] Anand, C. (2026, February 12). Summit AI's rural cyber blindside: Voice-cloned scams exploding in India's digital heartland. The Tech Panda. https://thetechpanda.com/summit-ais-rural-cyber-blindside-voice-cloned-scams-exploding-in-indias-digital-heartland/43952/

2.2.4 Android Malware and Device-Level Exploitation

While social engineering remains the dominant vector, a parallel technical infrastructure has matured around Android malware designed specifically for Indian banking users.

A popular campaign is FatBoyPanel, identified by the cybersecurity firm Zimperium in February 2025. In this campaign, approximately 900 malware samples were distributed through 1,000 malicious applications, all attributed to a single threat actor. The malware was distributed via text messaging platforms as APK files masquerading as government or banking applications. It intercepts OTPs, phishes identity documents, hides its icon from the home screen, disables Google Play Protect, and resists uninstallation. Attacker phone numbers were traced primarily to West Bengal, Bihar, and Jharkhand, which together accounted for 63% of the total.[24] [25]

Other active malware families include DogeRAT, an open-source Android remote access trojan distributed as fake applications and sold on text messaging platforms for as little as ₹ 2,500. In this case, a Bot functions as its command-and-control panel. These remote access trojans remain central to digital arrest scams, where victims are socially engineered into installing applications that give remote access to their devices.[26]

2.3
The Geopolitics of Fraud

India's cyber fraud landscape is no longer confined to domestic infrastructure or local criminal networks. A significant share of high-volume scams now originates from organised scam compounds across parts of Southeast Asia. These operations have turned online fraud into a cross-border supply chain that combines recruitment, confinement, and call centre-style execution, with Indian victims often targeted by individuals who were themselves lured abroad and then forced to participate in scams.

The recruitment pipeline typically begins with fake job offers circulated through social media. These roles are presented as customer support, data entry, sales, or IT work, with travel and accommodation arranged upfront to reduce suspicion. Once recruits arrive, passports and phones may be confiscated, movement restricted, and those who resist are subjected to threats. They are then pushed into meeting daily production targets that involve impersonation scripts and conversion tactics across multiple scam formats.

The core hubs remain clustered around border and special-zone geographies where legal enforcement is difficult. News reports continue to identify large compound clusters in Myanmar's border areas near Thailand, including sites such as KK Park and Shwe Kokko. Recent investigations also highlight how these operations maintain resilience through redundant connectivity, including the use of satellite internet terminals that allow scams to continue even when local controls tighten.[27]

---

[24] FatBoyPanel Android malware targets millions in India. (2025, May 7). Ampcus Cyber. https://www.ampcuscyber.com/shadowopsintel/fatboypanel-android-malware-campaign-targeting-millions-of-indian-users/
[25] Zimperium. (2025, January 31). Mobile Indian cyber heist: FatBoyPanel and his massive data breach. https://zimperium.com/blog/mobile-indian-cyber-heist-fatboypanel-and-his-massive-data-breach
[26] Das, A. (2023, May 29). DogeRAT: The Android malware campaign targeting users across multiple industries. CloudSEK. https://www.cloudsek.com/blog/dogerat-the-android-malware-campaign-targeting-users-across-multiple-industries
[27] Associated Press. (2024, November 15). Myanmar scam hubs detainees repatriation. AP News. https://apnews.com/article/myanmar-scam-hubs-detainees-repatriation-e4d814fecf29b4da56dc81cc8ec096c5

International researches and studies in 2025 describe these scam compounds as an industry that has matured into a modular criminal economy. The UN Office on Drugs and Crime has described the region as reaching an inflection point, where crackdowns in one geography push operators to relocate and replicate the model elsewhere. News reports tied to this research also note expansion beyond East and Southeast Asia, with scam infrastructure and operations increasingly appearing in Africa and parts of Latin America. Adding to the above, Myanmar's periodic crackdowns gives us a good idea of the limits of episodic enforcement against a system that is both profitable and politically protected. [28]

A pivotal moment to the above, came on October 20, 2025, when the Burmese military raided KK Park in Myawaddy, Kayin State, detaining over 2,000 workers and seizing more than 30 Starlink satellite terminals.[29] SpaceX announced that it had proactively identified and disabled over 2,500 Starlink Kits in the vicinity of suspected scam centres in Myanmar. The raid, however, quickly revealed its limitations. Three days later, KK Park was bombed by the Karen National Army, a Buddhist ethnic army, and approximately 1,500 workers fled across the Moei River into Thailand's Mae Sot, including hundreds of Indians and citizens of China, the Philippines, Vietnam, Ethiopia, and Kenya.[30]

At the same time, other investigations and satellite based reports suggest scam activity still resides despite demolitions and media announcements, with workers and equipment shifted across sites and networks. Satellite imagery analysis by C4ADS found that 14 of 21 known compounds in Myawaddy Township had shown construction or expansion since January 2025, including KK Park itself before the raid. KK Park is one of approximately 30 scam compounds along Myanmar's border with Thailand alone, and the Karen National Army control some 40 compounds along a 200 kilometer stretch hosting between 50,000 and 100,000 people.[31]

An interesting link to the above is that of Starlink, which had enabled these scam compounds to function effectively. Analysis of internet routing data by APNIC shows that Starlink went from negligible Myanmar traffic before February 2025 to ranking as the top internet provider every day from July 3 to October 1, 2025. This is despite SpaceX's claim of disabling 2,500 kits. Investigation by the Associated Press and PBS Frontline found at least two compounds continued using Starlink after the announced cutoff. A United States Congressional Joint Economic Committee investigation into Starlink's involvement has also been launched.[3233]

Cambodia has emerged as the second major epicentre of the scam compound economy, and has attracted unprecedented international enforcement action. An Amnesty International report published in June 2025, titled *'I Was Someone Else's Property,'* documented at least 53 scamming compounds across Cambodia with evidence of slavery, trafficking, child labour involving children as young as 14, and torture. The report accused the Cambodian government of deliberately ignoring abuses.[34] Following the

---

[28] United Nations Office on Drugs and Crime. (2025, April). Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia (Technical Policy Brief). UNODC Regional Office for Southeast Asia and the Pacific. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

[29] Myanmar military raids notorious KK Park scam compound, detaining thousands. (2025, October 21). The Guardian. https://www.theguardian.com/world/2025/oct/21/myanmar-kk-park-raid-scam-cybercrime-centre-compound

[30] Starlink, utilised by Myanmar scam centres, sees usage fall nationwide. (2025, November 12). BBC News. https://www.bbc.com/news/articles/cpd2e5541d1o

[31] Myanmar declares a 'zero tolerance' policy for cyberscams. But the fraud goes on. (2025, December 17). PBS Frontline. https://www.pbs.org/wgbh/frontline/article/myanmar-cyberscam-scam-compound/

[32] Myanmar scam centres using Starlink technology continue to thrive despite crackdown. (2025, October 14). ETTelecom (Economic Times). https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/myanmar-scam-centres-using-starlink-technology-continue-to-thrive-despite-crackdown/124541919

[33] US Congress committee investigating Musk-owned Starlink over Myanmar scam centres. (2025, October 14). The Guardian. https://www.theguardian.com/world/2025/oct/14/us-congress-committee-investigating-musk-owned-starlink-over-myanmar-scam-centres

[34] Amnesty International. (2025, June 26). Cambodia: 'I was someone else's property': Slavery, human trafficking and torture in Cambodia's scamming compounds (ASA 23/9447/2025). https://www.amnesty.org/en/documents/asa23/9447/2025/en/

report's publication, Prime Minister of Cambodia, Hun Manet, ordered a crackdown, and by mid October 2025, nearly 3,455 suspects had been detained in raids across 92 compounds in 18 cities.[35]

The most consequential action came from outside Cambodia. On October 14, 2025, the United States and the United Kingdom imposed, as stated by them, the largest sanctions action ever targeting a cyber fraud network in Southeast Asia. The action targeted 146 entities within the Prince Group Transnational Criminal Organisation led by Chen Zhi, a Chinese Cambodian national. The Department of Justice unsealed a 26 page indictment charging Chen Zhi with wire fraud and money laundering conspiracy, and filed the largest forfeiture action in United States history, totaling approximately 127,271 Bitcoin valued at roughly $15 billion.[36]

The United Nations Office on Drugs and Crime confirmed in its April 2025 report that scam infrastructure and operations are increasingly appearing in Africa, the Middle East, and Latin America. Nigeria has emerged as a hotspot, with the Economic and Financial Crimes Commission arresting 792 suspects including 193 Chinese, Arab, and Filipino nationals running crypto and romance scams.

Chinese organised crime networks remain the controlling architecture of the scam compound economy. The so-called Four Families of Kokang, the Bai, Liu, Wei, and Ming, built over 100 industrial compounds in northern Myanmar. Eleven members of the Ming family were sentenced to death by the Wenzhou Intermediate People's Court in September 2025 and executed on January 29, 2026, followed by four more executions on February 2, 2026.[37] China has repatriated more than 53,000 Chinese suspects from northern Myanmar compounds and claims its police solved 258,000 telecom fraud cases in 2025.[38] She Zhijiang, the Chinese Cambodian businessman who created Yatai New City at Shwe Kokko in partnership with militia commander Saw Chit Thu and the Karen National Army, was extradited from Thailand to China in November 2025. Adding to the above, The United States Treasury sanctioned Saw Chit Thu and the Karen National Army on May 5, 2025 as a transnational criminal organisation.[39]

For India, the most visible consequence has been the scale of rescues and repatriation. In a December 2025 written response in Parliament, the Government of India stated that over 6,700 Indian nationals have been rescued from scam and fake job rackets in Cambodia, Lao PDR, and Myanmar, with a country wise split that places Cambodia, Lao PDR, and Myanmar in the same broad range.[40]

The scale of the underlying crisis, however, is far larger than the rescue figures suggest. Open source intelligence indicates that between January 2022 and May 2024, at least 29,466 Indians travelled to Cambodia, Thailand, Myanmar, and Vietnam on tourist visas and never returned. Between January 2024 and November 2025, 16,127 complaints were received from Indian nationals abroad through the government's MADAD and CPGRAMS portals. Many of these cases involve individuals trapped in compounds run by Chinese organised crime networks. News reports from northeastern India have documented how Indians held in Myanmar compounds were rescued from sites operated by Chinese

[35] Cambodia arrests 3,455 online scam suspects in nearly 4 months. (2025, October 16). Xinhua News Agency. https://english.news.cn/asiapacific/20251016/65583fae8c884ce39d64eca3e9d52fec/c.html
[36] U.S. Department of the Treasury. (2025, September 25). U.S. and U.K. take largest action ever targeting cybercriminal networks in Southeast Asia (Press Release SB0278). https://home.treasury.gov/news/press-releases/sb0278
[37] China executes 11 members of Myanmar scam mafia. (2025, January 30). BBC News. https://www.bbc.com/news/articles/cx2qdrvy9qjo
[38] China solves 258,000 telecom, online fraud cases in 2025. (2026, January 8). Xinhua News Agency. https://english.news.cn/20260108/3f1e292d6b1b4e499b8b88db5dff984f/c.html
[39] U.S. Department of the Treasury. (2025, May 5). Treasury sanctions Burma warlord and militia tied to cyber scam operations (Press Release SB0129). https://home.treasury.gov/news/press-releases/sb0129
[40] Over 6,700 Indians, lured by scam centres, rescued from Cambodia, Myanmar. (2025, July 31). NDTV. https://www.ndtv.com/india-news/over-6-700-indians-lured-by-scam-centres-rescued-from-cambodia-myanmar-9794001

syndicates, with passports confiscated and workers forced to meet daily fraud targets under threat of physical violence.[41]

2.4 The Current Institutional and Regulatory Response and the Emerging Role of AI

India's response to rising cyber fraud has expanded across institutions, and this response now includes national reporting systems, regulatory mandates, and attempts to improve coordination across agencies. AI is also being used more and more to reduce the fraud response timeline, and this is changing fraud detection from retrospective investigation to live risk signaling and interception in high velocity payment systems. This is mainly due to the fact that machine learning based anomaly detection can support real time monitoring across transaction streams where manual review cannot work at this scale.

The steps taken by different Indian government departments point to a three-layer structure. First, the MHA, through the I4C, has expanded national systems for reporting, blocking, and intelligence sharing. These systems generate the data that AI systems need, and they also create the operational channels through which risk signals can be acted on quickly. Second, the RBI has publicly described a move beyond traditional rule-based detection, with a shared mule account detection model deployed across banks, along with ongoing work to explore transaction level risk scoring for digital payments. Third, the DoT has put in place telecom to finance signaling through a risk indicator for mobile numbers, backed by an integration advisory to banks and early reports of loss prevention within a short period.

2.4.1 National Reporting and Helpline Architecture

India has put in place a central reporting framework to support a faster response to cyber fraud, and this framework is anchored in the I4C under the MHA. One key part of this framework is the toll-free helpline 1930, which was created to support immediate reporting of financial cybercrime. When a fraud takes place, including when a person realises that they have been tricked into sending money, they can call 1930. The call is then routed to a state cyber police helpdesk that is connected to a pan India system.

In parallel, the MHA runs the NCRP, an online platform where the public can file complaints with incident details. The phone and portal channels feed into a unified backend, the CFCFRMS operated by I4C. The aim of this framework is to create real time alerts once a complaint is registered. If a victim reports that ₹50,000 was siphoned through UPI, the system can flag the beneficiary account and trigger coordination between law enforcement and bank fraud teams to freeze funds before they disappear.

Available secondary data by the government reflects measurable impact of the above architecture. Complaints through 1930 and NCRP helped freeze or recover more than ₹5,489 crore in 2024 alone. That was achieved by acting on about 17.8 lakh complaints during the year, indicating the scale of alerts being handled.[42] Each alert can trigger inter bank coordination to block transactions in transit or hold

[41] Sharma, Y. (2025, November 7). Sold for $5,000, nails pulled out—Indians' accounts of being trapped in Myanmar's cyber scam hubs. ThePrint. https://theprint.in/diplomacy/sold-for-5000-nails-pulled-out-indians-accounts-of-being-trapped-in-myanmars-cyber-scam-hubs/2780342/

[42] Press Information Bureau. (2025, October 8). "I dream of a Digital India where cyber security becomes an integral part of our national security" - Prime Minister Narendra Modi [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146

suspicious accounts, creating time for the victim. Speed is central to this as banks often have only a short window to reverse a fraudulent transfer. The 24x7 channel improves the chance of intercepting funds in motion. A good example is that of how Mumbai Police used the helpline to block ₹1.49 crore across 100 cases in 24 hours, highlighting what rapid reporting can do in practice. The portal also routes complaints digitally to the relevant jurisdiction, reducing delays linked to manual filing.[43]

The architecture also supports intelligence and disruption. I4C aggregates cyber fraud incident data in a way that enables broader actions. Coordination with the Department of Telecom has led to blacklisting of over 9.42 lakh SIM cards and 2.63 lakh device International Mobile Equipment Identity (IMEI) numbers linked to fraud.[44]Blocking these resources makes it harder for scam call centres and text messaging based fraud to reach new victims, and it increases pressure on KYC enforcement in SIM issuance.

A newer component is the Suspect Registry introduced in late 2024. It is a centralised database of fraud identities, mule accounts, and phone numbers compiled from cybercrime reports nationwide. In a short period, it reportedly collected over 11 lakh suspect identifiers and flagged more than 24 lakh bank accounts as known mule accounts. Banks can use this registry to avoid onboarding repeat offenders. Police can also prioritise frequent offenders. The registry reportedly prevented an estimated ₹4,631 crore in additional fraud by enabling earlier detection of transactions involving flagged mule accounts. This approach aims to convert reporting data into prevention by creating feedback loops where information from one case helps stop others.[45]

Public awareness and accessibility are also part of the system. The helpline has been promoted through CyberDost outreach and bank advisories. The intent is to make calling 1930 an immediate step after a fraud is detected. The portal also offers a Check Suspect tool that allows users to input a phone number, UPI ID, or bank account to see whether it has been reported previously, enabling basic reputational checks before transacting.

Overall, the helpline, portal, and analytic systems represent an effort to standardise reporting and create a unified response. Challenges persist, but the core architecture now resembles a modern hotline and reporting system that can act quickly when victims report in time.

2.4.2 Reserve Bank of India and Bank Level Initiatives

The RBI, as the banking and payments regulator, has responded to cyber fraud by tightening fraud risk management requirements and pressing banks to strengthen defenses. In July 2024, RBI issued revised Master Directions on Fraud Risk Management for banks and financial institutions, updating earlier guidance. The revised directions position fraud prevention as a board level priority. They assign explicit accountability to boards and senior management for oversight, and they require robust frameworks for early warning signals, real time monitoring, and prompt reporting.[46]

---

[43] Rs 1.49 cr seized in over 100 cases of cyber frauds within 24 hours of complaint on helpline '1930'. (2025, March 22). ThePrint. https://theprint.in/india/rs-1-49-cr-seized-in-over-100-cases-of-cyber-frauds-within-24-hours-of-complaint-on-helpline-1930/2560925/

[44] Nine lakh SIMs blocked, Rs 5.5K crore saved in cyber fraud war. (2025, July 23). The Economic Times. https://economictimes.indiatimes.com/news/india/nine-lakh-sims-blocked-rs-5-5k-crore-saved-in-cyber-fraud-war/articleshow/122866097.cms

[45] Sansad TV. (2025, August 12). Perspective: Rise in cyber fraud in India. https://sansadtv.nic.in/episode/perspective-rise-in-cyber-fraud-in-india-12-august-2025[Video]

[46] Reserve Bank of India. (2024, July 15). Master directions on fraud risk management in commercial banks (including regional rural banks) and all India financial institutions (RBI/DOS/2024-25/118). https://rbidocs.rbi.org.in/rdocs/notification/PDFs/118MDE97B8ED9A09B4B21BE7FDDE5F836CD09.PDF

The directions also signal a shift from a reactive approach, where fraud was often addressed only after detection, to a preventive model. A key procedural change is removal of the earlier ₹1 lakh threshold for reporting. Banks now need to record and report all fraud incidents, not only those above a value cut off. The rationale is that many cyber frauds involve numerous low value transactions that add up to large losses if patterns are missed.

RBI also strengthened expectations around root cause analysis and pattern recognition. Banks are expected to identify modus operandi and address systemic weaknesses rather than treating each incident in isolation. The revised directions also highlight money mules as a central risk vector. RBI has instructed banks and NBFCs to take proactive steps to detect and remove mule accounts from their customer base. This aligns with law enforcement assessments that mule accounts are critical to laundering and rapid fund movement.

Technology adoption has become a prominent part of the response. One initiative is the use of AI driven fraud detection tools. In late 2024, the RBI Innovation Hub developed MuleHunter.AI, a model designed to identify mule accounts at scale using machine learning on transaction data. The tool analyses 19 distinct behavioural patterns to detect mule accounts and reportedly flags approximately 20,000 mule accounts per month.[47] However, transparency remains a concern, as the RBI declined to share effectiveness data via RTI, citing fiduciary capacity with banks. A broader platform, the DPIP, was launched by RBI in 2025. Built by the Reserve Bank Innovation Hub, it provides AI-driven real time fraud detection by integrating telecom data, I4C intelligence, and banking fraud databases. The Indian Digital Payments Intelligence Company (IDPIC), a Section 8 company, was approved in December 2025 to operate DPIP.[48]

Beyond domestic initiatives, global payment networks have also begun supporting the fight against cybercrime. For example, in 2024, a Memorandum of Understanding (MoU) between the CERT-In and a global payment network was signed, which covered incident response, capacity building, and sharing of financial sector threat intelligence.[49]

Banks have also expanded anomaly detection systems. These tools can automatically flag or decline transactions that diverge from a customer's normal behavior, such as unusually large transfers to new payees at unusual hours. Such systems may trigger additional verification steps or temporary blocks.

RBI has also pushed cross sector integration. In mid-2025, the RBI issued an advisory making it mandatory for banks to integrate with the FRI developed by the Department of Telecommunications. This telecom to banking linkage is intended to stop fraud at the point of transaction by reducing the ability of scam operators to reuse the same numbers across victims. The full mechanics of the FRI, including its risk tiers, data inputs, and early results, are discussed in Section 2.4.3.[50]

In addition to the above, the RBI's Payments Vision 2028, released on 27 March 2026, proposes a Cyber Key Risk Indicators (KRI) framework specifically for non-bank Payment System Operators such as PhonePe, Google Pay, Paytm etc. The framework is designed to enable consistent risk specific IT supervision of these entities, allowing the regulator to compare cyber resilience across operators and generate early warning signals for potential IT and cyber risks before they transform into incidents. The

[47] Reserve Bank Innovation Hub. (n.d.). MuleHunter.AI. https://rbihub.in/projects/mulehunter
[48] Angel One. (2025, December 11). SBI, Bank of Baroda secures RBI approval to form Section 8 firms for digital payments intelligence platform. https://www.angelone.in/news/stocks/sbi-bank-of-baroda-secures-rbi-approval-to-form-section-8-firms-for-digital-payments-intelligence-platform
[49] Press Information Bureau. (2024, June 19). Two entities will leverage their shared expertise to strengthen financial sector cybersecurity incident response [Press release]. Ministry of Electronics & IT. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2026677
[50] Press Information Bureau. (2025, July 2). Department of Telecommunications welcomes RBI advisory on Financial Fraud Risk Indicator [Press release]. Ministry of Communications. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2141616

need for the same arose from the fact that the Payment System Operators, in spite of carrying a very large share of retail digital payment volumes in India, historically sat outside the more granular cyber supervision applied to scheduled commercial banks. The Payments Vision 2028 also proposes a shared responsibility framework in which both the issuing bank and the beneficiary bank jointly bear liability for unauthorised digital payment transactions, which, if implemented, would strengthen incentives for fraud prevention at both ends of a transaction rather than concentrating liability only at the remitter's bank.[51]

Consumer liability norms remain part of the regulatory baseline. Banks must follow RBI guidance on zero liability and limited liability for customers in unauthorised electronic transactions, depending on how quickly the customer reports. This increases the incentive for banks to strengthen authentication systems such as two factor authentication, biometric logins, and behavior-based verification. Banks have also increased customer awareness campaigns through SMS advisories, safe banking ads, and coordination with law enforcement.

Operationally, banks now often maintain dedicated fraud risk teams and nodal officers who can respond to CFCFRMS alerts at any hour to freeze accounts quickly. Industry actors such as NPCI have also introduced product level safeguards, including delays on new payee activation and risk scoring based warnings during UPI flows, such as alerts when receiver identity details appear suspicious. Coordination forums, including interbank advisory groups and incident response drills supervised by CERT In and RBI, also form part of the ecosystem.

Recently, the RBI opened a formal consultation on additional safeguards in digital payments through a Discussion Paper released by the Department of Payment and Settlement Systems. The paper sets out four options for stakeholder feedback, which include a mandatory one-hour lag at the payer's end for authorised push payment transactions above ₹10,000, an additional authentication by a trusted person for high value transactions initiated by citizens aged 70 and above and persons with disabilities, a ceiling on annual aggregate credits into accounts that have not undergone additional review of business relationship, and customer induced controls including a single kill switch to disable all digital payment channels from an account at one stroke.[52]

Overall, RBI and banks have moved across regulations, technology deployment, and inter agency collaboration. The direction of travel is toward faster detection, earlier blocking, stronger KYC controls to reduce fake account creation, and more aggressive customer education.

2.4.3 Department of Telecommunications controls over numbers, devices, and fraud signalling

The Department of Telecommunications has leaned into a practical insight i.e. a large share of scams are enabled by disposable numbers, SIM based identity abuse, and the ability to re contact victims at scale. Its citizen-facing platform, Sanchar Saathi, sits at the centre of this approach, combining device and connection level tools that reduce reuse of compromised identifiers. The platform, whose mobile application was launched on January 17, 2025, has facilitated termination of over 3 crore fraudulent mobile connections, blocking of 5.5 lakh handsets, and disabling of 16.97 lakh text messenger accounts. Beyond enforcement, Sanchar Saathi has also enabled recovery of 9.08 lakh stolen or lost mobile phones

[51] NewsOnAir. (2026, March 27). RBI announces its 'Payments Vision 2028', outlining roadmap to strengthen & expand India's rapidly growing digital payments ecosystem. Prasar Bharati. https://www.newsonair.gov.in/rbi-announces-its-payments-vision-2028-outlining-roadmap-to-strengthen-expand-indias-rapidly-growing-digital-payments-ecosystem/

[52] Reserve Bank of India. (2026, April 9). Exploring safeguards in digital payments to curb frauds (Discussion Paper). Department of Payment and Settlement Systems. https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/DP090420261ED5D6E68D724A6EA870B7E68E45F80F.PDF

and the disconnection of 2.41 crore unauthorised mobile connections after citizens flagged them through the portal's "Not My Number / Not Required" feature.[53]

One track within the Department focuses on citizen reporting of suspicious communications including calls, SMS, and messaging channels, creating a pipeline of actionable fraud signals for telecom enforcement. This reporting stream also feeds intelligence into risk scoring systems used by other parts of government and by private platforms. These signals flow into the Digital Intelligence Platform (DIP), a secure ecosystem for real time intelligence sharing designed to prevent telecom misuse in cybercrime and financial fraud. Over 1,200 organisations have been onboarded onto DIP, including central security agencies, police departments of all 36 States and Union Territories, banks, UPI providers, payment operators, and telecom service providers.

A second track focuses on lost or stolen devices and IMEI level blocking through the Central Equipment Identity Register (CEIR), which reduces the resale and reuse value of stolen phones and can also limit the ability of fraud actors to recycle devices across operations, particularly essential for scam ecosystems that operate with semi-industrial infrastructure, including device farms, multi-SIM setups, and quick churn across hardware.

A separate technical intervention targets international spoofed calls. The Calling Line Identity-based International Incoming Spoofed Calls Prevention System (CIOR), detects and blocks international calls that display Indian mobile numbers, a tactic commonly used by fraudsters impersonating government officials in digital arrest scams. Since its launch on October 17, 2024, CIOR has blocked up to 1.35 crore spoofed calls in a single day and has achieved an approximately 99 percent reduction in spoofed calls carrying Indian calling line identities.[54]

The most policy significant DoT initiative for financial fraud prevention is the FRI. DoT describes FRI as a risk-based metric that classifies mobile numbers as Medium, High, or Very High risk based on inputs that include National Cybercrime Reporting Portal reporting, Chakshu reports, and intelligence shared by banks and financial institutions. The institutional point is that FRI attempts to turn telecom side signals into decision grade indicators inside financial systems, so fraud can be interrupted closer to the point of transaction. FRI enables banks, NBFCs, and UPI platforms to trigger real time alerts, transaction delays, enhanced due diligence, and blocking measures against flagged numbers. Since May 2025, financial frauds worth over 1,500 crore rupees have been prevented through this mechanism.[55]

DoT has also expanded machine to machine sharing arrangements. The Digital Intelligence Unit shares a Mobile Number Revocation List (MNRL), which includes numbers disconnected due to cybercrime linkages, failed re verification, or misuse, and this dataset is explicitly referenced as an input into the broader fraud prevention ecosystem.

---

[53] Press Information Bureau. (2025, December 2). Launched in January 2025 to enhance transparent and secure mobile services [Press release]. PIB Headquarters. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2197871

[54] Press Information Bureau. (2026, February 12). Digital Intelligence Platform driving decisive action against telecom frauds: Shri Jyotiraditya Scindia [Press release]. Ministry of Communications. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2227052

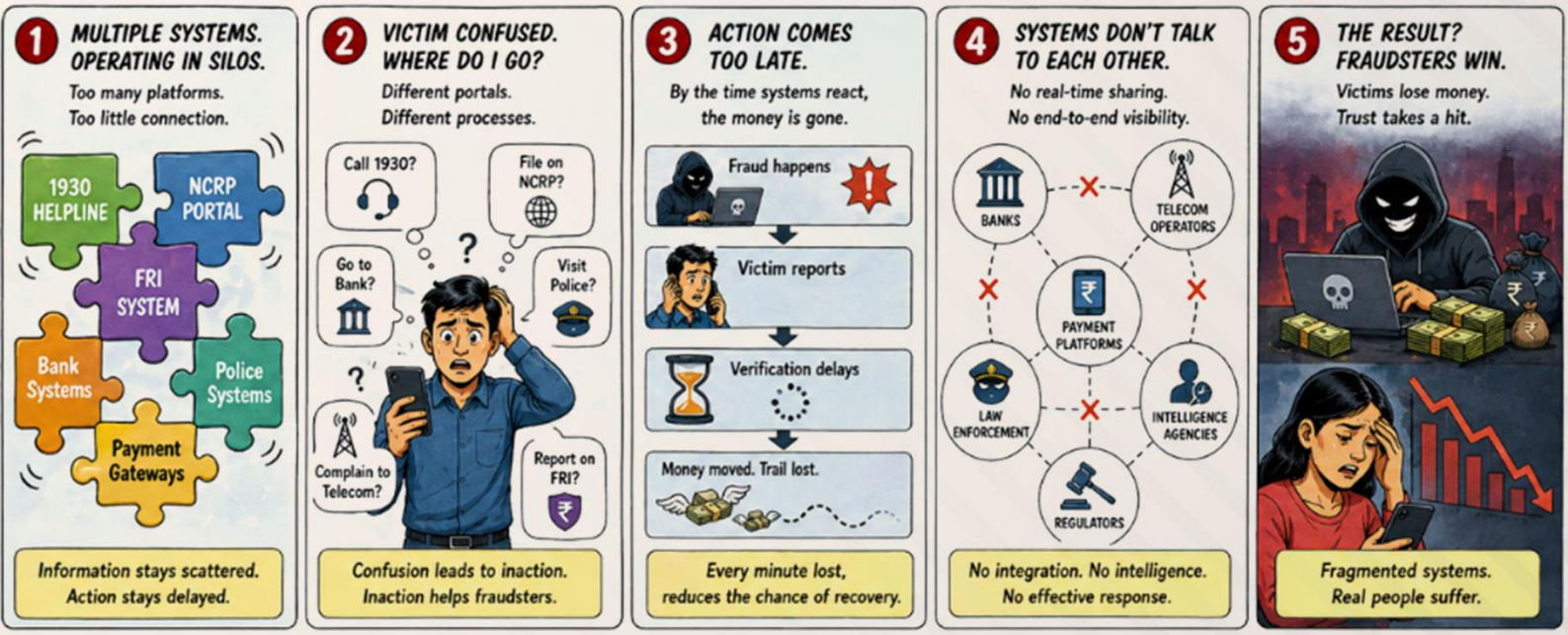
[55] Press Information Bureau. (2025, December 22). Financial Fraud Risk Indicator (FRI) of DoT helps prevent ₹660 crore cyber fraud losses in just 6 months [Press release]. Ministry of Communications. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2207376

A further step toward formal coordination is the September 2025 MoU between DoT and FIU IND, which frames automated exchange of MNRL data and suspicious mobile number signals linked to money mule activity, using DoT platforms and FIU IND's Finnex 2.0 portal. DoT has supplemented these technical and institutional measures with mass awareness and capacity building efforts.[56]

[56] Press Information Bureau. (2025, September 25). Real-time financial fraud risk data exchange set to boost cybersecurity efforts [Press release]. Ministry of Communications. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2171135

3.

Systemic Gaps in Prevention, Detection, and Redress



A standard UPI payment can be completed in as few as four to five taps, taking under ten seconds. This speed, the core Unique Selling Proposition of UPI, is simultaneously its greatest achievement and its greatest vulnerability.

Until June 2025, the pre transaction confirmation screen was able to display names extracted from QR codes or user set nicknames. Scammers routinely exploited this by embedding fraudulent names. The NPCI addressed this through Circular 101A/2025-26, effective June 30, 2025, which mandated that all UPI apps display only the registered bank name of the beneficiary. NPCI also introduced risk-based alerts on flagged transactions, though the specific details of these interventions have not yet been revealed. Recently, the person-to-person collect request feature, routinely exploited by fraudsters tricking users into approving outgoing payments disguised as incoming transfers, was banned effective October 1, 2025. In addition to the above preventive measures and safeguards, a four-hour cooling off period now limits new device registrations to ₹5,000 for the first 24 hours.[57]

These are meaningful incremental improvements, however they still leave some critical vulnerabilities untouched, such as no mandatory cooling off period exists for routine UPI person-to-person transfers, even for large amounts to first time recipients, and similarly no system triggers a human check or third party notification when successive large transfers occur within hours. A LocalCircles survey in 2025 found that one in five UPI using families experienced fraud since 2022, with more than half of victims not filing any complaint, suggesting that both warnings and redress mechanisms are failing at scale.[58]

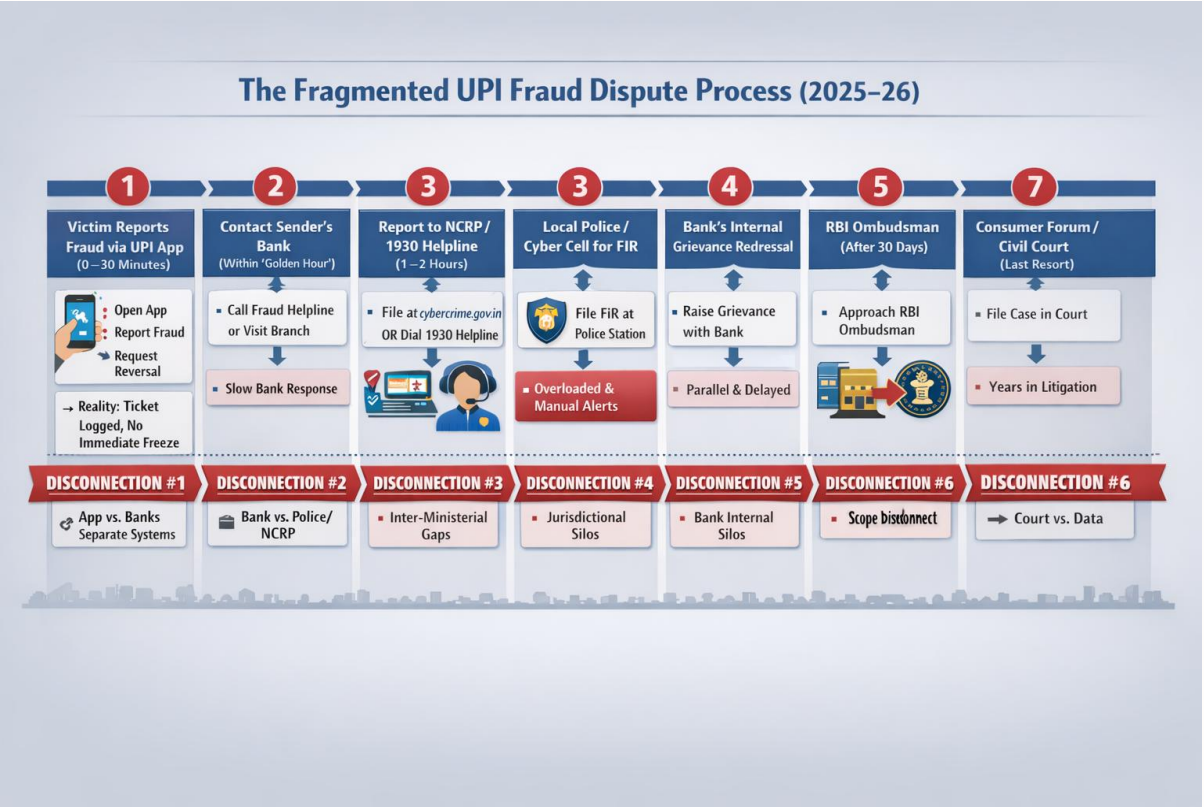
The intervention that actually saves victims is almost always human contact. In nearly every documented case, the scam ended when a family member or friend physically intervened. The scam's isolation tactic exists to prevent this. Yet no payment system attempts to replicate this intervention through an automated call to a trusted contact, a notification to a family member, or a mandatory delay that creates space for external reality to intrude.

3.1 What Users Face after the Scam

When a fraud victim in India seeks help, they have to navigate a number of disconnected institutions. The typical reporting journey requires engaging with several entities, starting first with the UPI app's internal dispute mechanism, then the sender's bank, the NCRP, the local police or cyber cell for a First Information Report (FIR), the bank's internal grievance mechanism, the RBI Ombudsman if the bank fails to resolve within 30 days, and potentially a consumer forum if all else fails. Each entity maintains separate tracking systems with no interoperability, requires its own documentation, and operates on its own timeline.

[57] PwC India. (2025, October). The Indian payments handbook 2025-2030 (6th ed.). https://www.pwc.in/assets/pdfs/indian-payments-handbook-2025-2030.pdf

[58] LocalCircles. (2025, June 26). 1 in 5 families surveyed that have someone using UPI confirm experiencing UPI fraud once or more in the last 3 years; 51% of them did not file any complaint, anywhere. https://www.localcircles.com/a/press/page/upi-fraud-complaint



The 1930 helpline, a frontline interface between victims and the response system, has been under sustained pressure as complaint volumes have climbed. Reports from users on public forums, including I4C's own social media channels, indicate that some victims have had to call repeatedly before reaching an operator, particularly during periods of peak inflow. These operational constraints appear to be a function of rapid demand growth rather than of any individual state or central agency, and they underline the case for the capacity and automation upgrades.

The NCRP has been scaling up against a sharp rise in demand. Incidents reported on the portal grew from about 4.52 lakh in 2021 to 22.68 lakh in 2024 and then to 28.15 lakh in 2025, which is roughly a sixfold increase over four years.[59] Users have at times reported slower portal response during high traffic periods and have asked for clearer updates on the status of their complaints, both of which point to the need for continued investment in portal capacity.

A Delhi High Court Public Interest Litigation filed in February 2026 sought the creation of a seamless integration linking the national cybercrime helpline portal with UPI apps, banks, payment service providers, and telecom operators.

3.1.1 Recovery Statistics

An interesting thing to note with regard to the statistics available is the gap between what the government reports as saved and what victims actually receive. IndiaSpend's analysis of NCRP data as of February 2025 reveals 3.8 million cyber fraud incidents reported, total losses of ₹36,448 crore, ₹4,381 crore placed under lien, but only ₹60.52 crore actually returned to victims. That is a return rate of 0.17%

[59] Press Information Bureau. (2025, October 8). Cybersecurity incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024 [Press release]. PIB Headquarters. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146

of total reported losses.[60] The government's own figures, separately reported by the MHA to the Parliament, indicate that the CFCFRMS stopped approximately ₹7,647 crore in fraudulent transactions from April 2021 to November 2025.[61] However, saved means frozen or placed under lien, not returned. The MHA's January 2026 Standard Operating Procedure (SOP) was drafted precisely because this gap had become untenable, of ₹7,647 crore stopped, only ₹167 crore had been restored to victims, which amounts to 2.18%.[62]

The FIR conversion bottleneck exacerbates the problem. Of 28.15 lakh cybercrime cases reported in 2025, only 55,484 FIRs were filed, approximately 2% . Without an FIR, there is no formal investigation and no prosecution. In practice, police actively refuse FIRs.[63]

The RBI's 2017 circular on customer liability in unauthorised electronic transactions establishes a zero-liability framework for fraud reported within three working days where the customer is not at fault. Courts have upheld this strongly.[64] The Delhi High Court in *Hare Ram Singh v. RBI* in November 2024 held the State Bank of India liable for ₹2.6 lakh lost in a phishing attack, finding that the victim did not share OTPs and that the bank's two-factor authentication system was breached through malware that intercepted OTPs automatically. Justice Dharmesh Sharma ruled that the breach was attributable to SBI's failure to implement adequate security measures, constituting a deficiency in service, and directed compensation under the zero-liability framework. However, enforcement remains inconsistent, and banks frequently refuse refunds, citing customer negligence.[65]

A further dimension of institutional failure is the issue of account freezing. When police trace fraud funds through mule account chains, they routinely freeze all accounts in the money trail, including those of innocent people who received even small disputed amounts. In Raipur, over 50 people had accounts blocked over amounts ranging from ₹2,000 to ₹20,000. Similarly, in a recent Faridabad case, a single investigation resulted in the freeze of 36,000 bank accounts nationwide, with innocent individuals blocked over amounts as low as ₹826.[66] [67]

3.2 The Golden Hour and Latency of Response

The golden hour in cyber fraud response refers to the narrow window, typically one to four hours, during which stolen funds are most likely still accessible in the first receiving mule account before being layered

[60] IndiaSpend. (2025, August 28). Complaints rose fivefold since 2021, and digital payment and 'digital arrest' scams surged. https://www.indiaspend.com/data-viz/dataviz-how-indias-cyber-crime-incidence-is-rising-972933
[61] News18. (2026, January 27). Rs 7,647 crore blocked since April 2021, but only 2% of money lost in cyber fraud recovered: Govt. News18. https://www.news18.com/india/rs-7647-crore-blocked-since-april-2021-but-only-2-of-money-lost-in-cyber-fraud-recovered-govt-ws-l-9857665.html
[62] Ministry of Home Affairs. (2026, February 4). Prevention of cyber financial fraud (Rajya Sabha Unstarred Question No. 553). Government of India. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/RS04022026/553.pdf
[63] Insights on India. (2026, February 21). Cybercrime in India 2025: 24% spike, ₹22,495 crore lost. https://www.insightsonindia.com/2026/02/21/cybercrime-in-india/
[64] Reserve Bank of India. (2017, July 6). 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). https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336
[65] Delhi High Court. (2024, November 18). Hare Ram Singh v. Reserve Bank of India & Ors. (W.P.(C) No. 13497/2022). https://delhihighcourt.nic.in/app/showFileJudgment/61018112024CW134972022_190247.txt
[66] Dainik Jagran English. (n.d.). Raipur victims struggle as bank accounts frozen over fraud money: Over 50 cases reported. https://english.dainikjagranmpcg.com/states/chhattisgarh/raipur-victims-struggle-as-bank-accounts-frozen-over-fraud-money/article-9468
[67] The420.in. (n.d.). A ₹4.43-crore scam, 36,000 frozen accounts: How UPI fraud hit innocents. https://the420.in/faridabad-cyber-scam-upi-fraud-accounts-frozen-home-ministry/

across dozens of subsequent accounts. Haryana Police has publicly stated that reporting within the first hour on the 1930 helpline can yield recovery rates of 90 to 100%, dropping to approximately 60% within six hours and declining further to 20% beyond that window.[68] Gujarat Police has reported recovering over ₹147 crore within 15 months, with nearly 80% success in cases reported within eight hours. However, after 48 hours, recovery prospects collapse because mule accounts are kept active for only one to two days before being drained via bulk payouts, ATM withdrawals, cryptocurrency conversion, or cascading UPI transfers.[69]

The speed of money laundering through mule networks is extraordinary. Prior Investigation by the Enforcement Directorate has found that stolen funds are broken into smaller transactions of ₹1 to 5 lakh and transferred into hundreds of accounts within a single day. An investigation by the Madhya Pradesh State Cyber Cell traced funds through up to ten successive accounts, with ₹638 crore siphoned from approximately 64,000 victims through 2.93 lakh bank accounts.[70] Similarly, the CBI's Operation Chakra V in June 2025 identified 8.5 lakh mule accounts across 700 bank branches nationwide.[71]

The institutional response chain has to contend with this velocity across a large number of participating entities, and in several parts of the workflow it still relies on manual handoffs that were designed for a lower volume environment. The CFCRMS, which now connects over 85 banks and payment intermediaries, represents India's most ambitious attempt at a real time fraud response. When a victim calls 1930 or files a complaint on the NCRP, state police operators log the complaint, the system generates alerts to nodal officers at the relevant financial institutions, and banks are directed to freeze suspected amounts. The helpline handled approximately 3.24cr calls in 2025, reflective of the growth in reporting and the operational strain on the frontline response.[72]

Turnaround time on freeze and defreeze requests has emerged as a focus area within this chain. In November 2025 Cyberabad Police flagged cases where freeze orders and defreeze requests were taking longer than expected and directed participating banks in its jurisdiction to set up dedicated Cyber Crime Response Desks, which several banks have since done.[73] API integration between participating banks and the CFCRMS is also at different stages of maturity across the system. The MHA SOP issued in January 2026 sets the expectation that all participating banks will integrate with the NCRP through APIs and respond in real time, which provides a clear implementation direction for the next phase.

As highlighted above, UPI's instant settlement architecture also creates a uniquely challenging recovery environment. Unlike credit card transactions, which have formal chargeback mechanisms allowing dispute resolution over 30 to 120 days between issuing banks, acquiring banks, and card networks, UPI transactions are designed to be instant and irrevocable. A reversal can occur only if the beneficiary

[68] The Times of India. (2024, March 18). Dialling 1930 in 'golden hour' key step to tackle cyber cons. https://timesofindia.indiatimes.com/city/chandigarh/dialling-1930-in-golden-hour-key-step-to-tackle-cyber-cons/articleshow/108931577.cms

[69] The Indian Express. (2025, May 1). In 15 months, Gujarat Police recovered over Rs 147 crore lost to cyber fraud. Reporting within 8 hours the key, say officers. https://indianexpress.com/article/cities/ahmedabad/in-15-months-gujarat-police-recovered-over-rs-147-crore-lost-to-cyber-fraud-reporting-within-8-hours-the-key-say-officers-10009157/

[70] The420.in. (n.d.). MP: ₹638 cr cyber fraud, 3 lakh accounts frozen across 17 states. https://the420.in/mp-638cr-cyber-fraud-3lakh-accounts-frozen-17-states/

[71] The Hindu. (2025, October 8). Operation Chakra-V: CBI conducts searches across six states in 'digital arrest' case. https://www.thehindu.com/news/national/operation-chakra-v-cbi-conducts-searches-across-six-states-in-digital-arrest-case/article70140111.ece

[72] The New Indian Express. (2026, April 12). Cybercrime helpline 1930 logs 3.24 crore calls in 2025, nearly one every second. https://www.newindianexpress.com/nation/2026/Apr/12/cybercrime-helpline-1930-logs-324-crore-calls-in-2025-nearly-one-every-second

[73] The Hindu. (2025, November 28). Key concerns over delays in cybercrime response raised at bank coordination meeting. https://www.thehindu.com/news/cities/Hyderabad/key-concerns-over-delays-in-cybercrime-response-raised-at-bank-coordination-meeting/article70334640.ece

authorises their bank to do so, which is impossible when the beneficiary is a mule account controlled by a criminal network.

Tap to pay on a tokenised virtual card is worth noting as a practical alternative for everyday retail use. The user experience is effectively identical to UPI Tap and Pay, a single tap on an NFC enabled point of sale terminal, but the underlying rail inherits the chargeback protections of the card network. Therefore, a disputed transaction can be raised through a structured process between the issuing bank and the acquiring bank, which is the recourse mechanism that UPI's instant settlement does not currently provide. Device bound tokenisation also ensures that the actual card number is never shared with the merchant and cannot be reused outside the registered device. However, tap to pay via tokenised virtual cards does not solve authorised push payment fraud, since a user who is socially engineered into authorising a tap can still lose money, but it gives users a parallel rail that combines contactless convenience with the formal recourse that irrevocable UPI transfers lack.

Courts at multiple levels have observed that banks can be held liable for deficiency of service when they fail to act promptly on fraud alerts, noting the asymmetry between the speed of digital fund transfers and the pace of institutional response.

The RBI's draft compensation scheme, released on March 6, 2026, proposes coverage of 85% of the net loss or ₹25,000, whichever is lower, for fraud cases involving amounts below ₹50,000. The cost would be shared among the RBI at 65%, the customer's bank at 10%, and the beneficiary bank at 10%, with the victim bearing the remaining 15%. The scheme is proposed to take effect from July 1, 2026,

3.3 The Siloed Intelligence Problem

The underlying issue is structural. Each actor in India's digital payments ecosystem holds a distinct slice of the intelligence, such that, if combined, it could identify fraud before funds leave a victim's account. Banks hold transaction histories, KYC records, and account behaviour patterns. They can see when an inactive account suddenly receives and forwards large sums, but they cannot see whether the phone number associated with the sender has been flagged in hundreds of cybercrime complaints. Telecom providers hold call records, SIM registration data, and device IMEI information. They can see when a number is making hundreds of outbound calls from a SIM box, but they cannot see that those calls are triggering large UPI transfers within minutes. Law enforcement holds complaint data and suspect registries compiled from millions of reports, but cannot access live transaction streams to trace fund flows in real time. Payment platforms hold UPI metadata and merchant interaction patterns, but each operates within its own ecosystem with limited visibility into what other platforms observe.

The initiatives described in Section 2.4 were designed to bridge these gaps. The reality, however, is that integration remains partial and uneven. MuleHunter.AI, as of December 2025, has been implemented by 23 banks according to a Right to Information response. The same RTI revealed that the RBI does not hold information on formal coordination between MuleHunter and the I4C, suggesting that the model's outputs are not feeding into law enforcement intelligence.[74]

[74] MediaNama. (2025, December). RTI reveals 23 banks have implemented MuleHunter.AI initiative. https://www.medianama.com/2025/12/223-rti-23-banks-mulehunter-mule-accounts/

The FRI has shown measurable results, with approximately ₹660 crore in fraud losses prevented within six months of launch and over 1,000 banks and payment platforms connected to the DIP.[75] The limitation is in what happens after a flag is raised. Different banks adopt different policies for FRI flags. Some delay transactions involving high-risk numbers, while others display warnings but allow the payment to proceed. A few do nothing beyond logging the signal. There is no standardised protocol mandating a uniform response to a given FRI risk level. A mobile number classified as very high risk by the Department of Telecommunications may trigger a block at one bank and a soft warning at another. This results in inconsistent protection that depends on which bank or payment app the victim happens to use.

The Suspect Registry, now containing 18.43 lakh suspect identifiers and 24.67 lakh layer 1 mule bank accounts, has blocked ₹8,031 crore in fraudulent transactions.[76] These are prevention figures, however, and the conversion to victim recovery remains weak. The registry also raises a question about data freshness, as mule accounts are opened, used, and discarded within days. A registry that flags accounts after they have already been linked to complaints may arrive too late to prevent the next transaction, while simultaneously freezing accounts of innocent individuals who received small amounts in the interim.

The DPIP, approved in December 2025 through the IDPIC, represents the most comprehensive attempt at integrated fraud intelligence. RBI Deputy Governor T. Rabi Sankar described the vision as collecting information from multiple sources and training an AI system on this data to generate pre-transaction alerts. Phase 1 integrates a Negative Registry across telecom operators, I4C data, and banking fraud databases, with five banks initially onboarded. The platform's long-term promise is significant, but its current state is early. Full deployment across the banking system has no published timeline, and even the governance structure for data contribution and access across competing private institutions remains under development. Industry observers have cautioned that past efforts to create shared databases in India have been stalled by legal and commercial disputes, and DPIP faces similar risks if participation is not mandated and governance is not clarified quickly.[77]

Legal barriers worsen the technical fragmentation. The Prevention of Money Laundering Act prevents banks from independently freezing suspected mule accounts without court or law enforcement authorisation. This creates a critical time gap, where a bank that identifies suspicious activity through MuleHunter must wait for a law enforcement directive before acting, during which time the funds have already moved. The Indian Bankers' Association has formally urged the RBI to grant banks independent authority to freeze accounts flagged as mule accounts, a request that remained unresolved as of early 2026.[78] Further, the Digital Personal Data Protection Act 2023 rejects legitimate interest as a lawful processing basis, which complicates the legal foundation for inter-institutional fraud data sharing. Banks and telecom providers sharing customer data for fraud prevention purposes operate in a grey area without explicit statutory protection, creating institutional reluctance to share aggressively. The MoU between the Department of Telecommunications and the Financial Intelligence Unit India, signed in September 2025, now provides a formal basis for automated exchange of mobile number revocation data and signals linked to money mule activity, and represents an important step toward institutionalising telecom to financial intelligence sharing. Building on this arrangement and extending it to other data flows will be central to closing the remaining gaps in cross sector fraud intelligence.

---

[75] Ministry of Communications. (2025, December 22). Financial Fraud Risk Indicator (FRI) of DoT helps prevent ₹660 crore cyber fraud losses in just 6 months [Press release]. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2207376

[76] Indian Cyber Crime Coordination Centre. (2025, December 10). Cyber digest (No. CD-763) [PDF]. Ministry of Home Affairs, Government of India. https://i4c.mha.gov.in/cyber_digest/dec_2025/Daily%20Digest-10.12.25.pdf

[77] The New Indian Express. (2025, October 1). RBI developing AI-driven tool to flag fraudulent transactions. https://www.newindianexpress.com/business/2025/Oct/01/rbi-developing-ai-driven-tool-to-flag-fraudulent-transactions

[78] MediaNama. (2025, April). IBA pushes for RBI power to freeze mule bank accounts. https://www.medianama.com/2025/04/223-iba-rbi-cyber-fraud-measures-freeze-bank-accounts-cybercrime/

Airtel Managing Director Gopal Vittal's June 2025 letter to over 40 banks, the RBI, and the NPCI reflected the frustration. He noted that existing systems are largely reactive and that Airtel possesses strong signals that could identify potentially fraudulent transactions, but that no mechanism exists for real-time telecom-to-finance signalling at the transaction level. He proposed a centralised fraud domain repository and a cross-sector fraud bureau.

3.4 Friction Points in Grievance Redressal

The Reserve Bank's Integrated Ombudsman Scheme, a centralised redressal mechanism for complaints regarding Banks and fintech entities, received 13.34 lakh complaints in the financial year 2024-25, a 13.55% increase over the prior year. The disposal rate was 93.07%, with an average turnaround of approximately 33 days. However, these figures mask a deeper concern. Of 9.11 lakh complaints received by the Centralised Receipt and Processing Centre, 7.76 lakh, or 85%, were classified as non-maintainable, falling outside the scheme's scope. This is indicative of a fundamental mismatch between what fraud victims expect from the ombudsman and what the system is designed to handle.[79]

The geographic distribution of complaints also reveals exclusion. Only 10.04% of complaints originated from rural areas in FY25, despite rural India comprising approximately 65% of the population. Metropolitan centres accounted for 45.86%, and 91.22% of complaints were filed digitally. The complaint system requires internet access, digital literacy, English language proficiency, and follow up over weeks, structurally excluding the populations most vulnerable to fraud.

However, as highlighted above, courts have intervened when the system fails. The Bombay High Court in *Jaiprakash Kulkarni v. Banking Ombudsman* in June 2024 overturned the ombudsman's rejection and directed Bank of Baroda to refund ₹76.9 lakh with 6% interest. Judicial relief, however, is accessible only to those with the resources and persistence to pursue litigation, which is a small fraction of India's fraud victims.[80]

India's federal structure adds another layer of friction, since cyber fraud routinely involves accounts across several states. An investigation initiated in Madhya Pradesh, for example, traced funds through accounts in Bihar, Uttar Pradesh, Jharkhand, Maharashtra, Rajasthan, Chhattisgarh, and West Bengal. In February 2026 a Public Interest Litigation filed in the Delhi High Court called for a multi-jurisdictional SOP and for an expansion of the e-Zero FIR framework to cover cyber financial frauds below ₹10 lakh. The e-Zero FIR, launched in May 2025, automatically generates a Zero FIR for cyber financial fraud complaints above ₹10 lakh, which in practice excludes the vast majority of retail digital payment frauds, including both UPI frauds and non UPI frauds routed through cards, wallets, Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT), and Real Time Gross Settlement (RTGS).

[79] Livemint. (2025, August 14). RBI Ombudsman saw 13% increase in consumer complaints in FY25: Here's how to resolve your grievances. https://www.livemint.com/money/personal-finance/rbi-ombudsman-saw-13-increase-in-consumer-complaints-in-fy25-heres-how-to-resolve-your-grievances-11764681127264.html

[80] Bombay High Court. (2024, June 14). Jaiprakash Kulkarni and Ors. v. The Banking Ombudsman and Ors. (Writ Petition No. 25600 of 2023) [2024:BHC-OS:8627-DB]. https://bombayhighcourt.nic.in

3.5
Structural and Institutional Drivers of Fraud Persistence

India's digital payment fraud ecosystem is resilient because the structural conditions enabling fraud remain largely intact. The core drivers form a reinforcing system, where weak identity verification enables mass mule account creation, abundant mule accounts enable rapid money laundering, rapid laundering defeats slow institutional response, low conviction rates maintain negligible deterrence, and economic vulnerability ensures a continuous supply of recruitable participants.

KYC failures remain the entry point because banks overwhelmingly treat KYC requirements as a regulatory checklist rather than an active fraud prevention mechanism. BioCatch's analysis of 350 million sessions at Indian banks found that 55% of sessions were operated by third parties, meaning accounts had been taken over or were being operated by someone other than the registered holder.[81] Additionally, the RBI Innovation Hub found that eight of ten banks surveyed still rely on simple rule-based systems to flag suspicious accounts.[82]

Enforcement capacity is also inadequate as India's police strength stands at 154 per 100,000 population against the United Nations recommended 222.[83] A Right to Information (RTI) response revealed that in Mumbai, out of 2,002 online financial fraud cases registered between 2021 and April 2025, there were just 2 convictions, a conviction rate below 0.1 per cent.[84] National Crime Records Bureau figures show approximately 2.05 lakh cybercrime FIRs registered between 2021 and 2023, against nearly 49 lakh cyber fraud complaints in the same period.[85] Adding to this, penalties under the Information Technology Act are disproportionate, where sections 66C and 66D provide for a maximum of three years imprisonment and ₹1 lakh fine for identity fraud and cheating by impersonation.

It is also important to note that the economics of mule recruitment fuel a seemingly inexhaustible supply chain. CloudSEK's investigation of the XHelper Android app revealed a fully gamified recruitment platform with ranking lists for mules to track earnings and compete, and training modules showing how to open fake corporate and merchant accounts. These networks follow pyramid-style referral structures with bonuses for successful recruitment. They also specifically target economically vulnerable populations in small towns, promising commissions for lending access to their accounts.[86]

[81] BioCatch. (2024). 2024 digital banking fraud trends in India [White paper]. https://www.biocatch.com/resources/white-paper/digital-banking-fraud-trends-india-2024
[82] Zigram. (2025). Understanding mule accounts in Tier 1 and Tier 2 cities in India. https://www.zigram.tech/article/mule-accounts-tier-1-tier-2-cities-india/
[83] Vision IAS. (2025, March 17). Law and disorder: States must spend more on adequate police forces. Business Standard summary. https://visionias.in/current-affairs/upsc-daily-news-summary/article/2025-03-17/business-standard/polity-and-governance/law-and-disorder-states-must-spend-more-on-adequate-police-forces
[84] Times of India. (2025, April 28). 2k cyber financial fraud cases in 4 yrs, just 2 convictions: RTI. https://timesofindia.indiatimes.com/city/mumbai/2k-cyber-financial-fraud-cases-in-4-yrs-just-2-convictions-rti/articleshow/120627760.cms
[85] The Federal. (2025). Digital arrest scams: Smarter fraudsters, lagging govt response? [AI With Sanket]. Dailyhunt. https://m.dailyhunt.in/news/india/english/the+federal+english-epaper-thefeden/digital+arrest+scams+smarter+fraudsters+lagging+govt+response+ai+with+sanket-newsid-n697642112
[86] CloudSEK. (2024, February 7). Shadow banking in your pocket: Exposing Android app used by money mules. https://www.cloudsek.com/blog/shadow-banking-in-your-pocket-exposing-android-app-used-by-money-mules

3.6 Technology Gaps and the Opportunity for AI

India's fraud detection infrastructure sits at the nascent stage of a technological transition it has not yet meaningfully undertaken. According to RBI survey data underpinning its Framework for Responsible and Ethical Enablement of AI (FREE-AI), only 21% of RBI-regulated entities utilise AI of any kind, with zero adoption among Urban Cooperative Banks and Asset Reconstruction Companies. Of the 127 entities using AI, only 15 employed interpretation tools like SHAP or LIME, and only 18 maintained audit logs. The remaining 79% of the regulated financial sector operates on rule-based transaction monitoring systems that generate false positive rates approaching 20%, declining legitimate transactions while sophisticated attacks slip through.[87]

In addition to the above, the RBI's FREE-AI Framework establishes seven guiding principles, and while these are constructive foundations, they remain guidelines rather than binding regulations with unclear implementation timelines. India has no unified AI regulatory framework comparable to the European Union's AI Act.

The most critical missing capability is a Confirmation of Payee system comparable to the United Kingdom's, where the payee's name is verified against bank records before payment execution, and the user is warned of mismatches. The UK system, expanded in October 2022, reduced investment scams by 20 per cent and impersonation scams by 30%. The Netherlands' IBAN Name Check produced a 70% drop in invoice fraud within nine months. NPCI's June 2025 mandate to display bank-registered beneficiary names is a partial step, but does not constitute an interactive verification system that warns users of mismatches before payment execution.[88]

India has already taken an important first step toward payee name verification across high value non-UPI rails. The RBI, through a circular dated 30 December 2024, has mandated a beneficiary bank account name look up facility for Real Time Gross Settlement and NEFT transactions, to be implemented by all participating banks by 1 April 2025. The facility fetches the beneficiary account name from the beneficiary bank's Core Banking Solution and displays it to the remitter before the transfer is initiated, extending to RTGS and NEFT the kind of name verification that was already available on UPI and IMPS.

However, the Indian facility is essentially a name display mechanism. The beneficiary bank returns the name on record and the remitter decides whether to proceed. On the other hand, the United Kingdom system returns a graduated response across four outcomes, which include a full match, a close match where the actual account holder name is surfaced for cross check, an explicit no match warning, and an unavailable response.

With regards to NPCI in particular, a pilot federated model with select banks combines banks' internal customer risk scores with NPCI's own transaction and device profiling scores, provided at no cost to banks. However, the deployment remains nascent. Most financial institutions still use fraud detection systems designed for card transactions, struggling with UPI's friction-less settlement architecture and volume of over 18.67 billion transactions in a single month.[89]

---

[87] Reserve Bank of India. (2025, May 29). Annual report 2024-25 [PDF]. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D5851.PDF

[88] BioCatch. (2023, November 14). History of Confirmation of Payee and its effectiveness against fraud. https://www.biocatch.com/blog/confirmation-of-payee-effective-against-fraud

[89] MediaNama. (2025, April 3). NPCI's AI-driven risk scoring to help banks combat UPI fraud. https://www.medianama.com/2025/04/223-npci-ai-upi-fraud-detection/

Graph and network analytics for detecting mule account rings are present in specific Indian deployments, including MuleHunter.AI and a small set of vendor tools used by individual banks, but they have not yet become standard practice across the banking system, which still relies predominantly on rule-based transaction monitoring as noted earlier in this section. The same gap is visible in transaction risk decisioning, where global payment networks have built mature systems that apply proprietary network data and machine learning models to score transactions in real time and help issuers approve more genuine payments while reducing false declines. Some of these systems now use generative AI techniques trained on global transaction flows to score transactions in milliseconds, a capability that Indian payment infrastructure has not yet replicated at scale.

Beyond transaction scoring, two further categories of tools are available to banks but remain underused in India. The first is payment ecosystem threat intelligence, which supplies banks with live information on card numbers being tested by fraudsters, merchant websites compromised by skimming code, and stolen card data surfacing on illicit marketplaces, allowing the bank to block or reissue affected cards before losses occur. The second is identity monitoring, which continuously scans breach databases and illicit forums for a customer's personal information and alerts them when it appears. Device intelligence and behavioural biometrics, which identify users through device fingerprints and typing or swipe patterns, are marketed to Indian banks by vendors such as Bureau.id, Callsign, and BioCatch, but adoption across the sector remains limited.

Data quality constraints also fundamentally limit AI deployment. Indian banks have to work with fragmented data across legacy systems storing information in outdated formats, with data silos sometimes worsened by new applications deployed without integration. Globally, 87% of banks cite data management as their biggest hurdle for AI adoption. In India, the challenges are compounded by the absence of standardised domain catalogs across banking terms, the scarcity of labelled fraud data, and concept drift as fraud tactics end up evolving faster than training data.

There are also some learnings from global best practices. For instance, Australia's Scam Safe Accord, backed by a $100 million industry investment in confirmation of payee, biometric verification for new accounts, and mandatory participation in intelligence sharing exchanges, produced a33% reduction in scam losses in its first full year.[90] Similarly, Singapore's ScamShield combines a government created AI consumer app with over 900,000 downloads and 120,000 scam entities blacklisted with the Shared Responsibility Framework imposing enforceable duties and liability on both financial and telecom institutions.[91] India's equivalent, the 1930 helpline and NCRP, lacks the integrated AI classifier, crowdsourced intelligence capabilities, and enforceable cross-sector liability of these systems.

3.6.1 Accessibility and Inclusion

India's fraud safeguards are designed, implicitly, for a literate, English speaking, urban smartphone user. The populations most vulnerable to fraud, including senior citizens, rural users, low literacy populations, persons with disabilities, and non English speakers, are precisely those least served by current protections.

Senior citizens are disproportionately targeted. In Nagpur, 60% of cyber fraud victims in 2025 were senior citizens, with ₹45.77 crore defrauded over the year.[92] In Goa, the share of senior citizens among

[90] America's Credit Unions. (2025, March 18). Australian credit unions achieve breakthrough results by separating fraud from scams. https://www.americascreditunions.org/blogs/americas-credit-unions/australian-credit-unions-achieve-breakthrough-results-separating-fraud

[91] Government Technology Agency of Singapore. (n.d.). ScamShield. https://www.tech.gov.sg/products-and-services/for-citizens/scam-prevention/scamshield/

[92] Nath, S. (2026, January 5). Cyber fraud drains ₹45.77 crore in 2025; 60% of victims senior citizens in Nagpur. The420.in. https://the420.in/nagpur-cyber-fraud-2025-senior-citizens-digital-arrest-scams/

cybercrime cases more than doubled from 6.17% in 2023 to 14.11% in 2024.[93] Rural and semi urban India has become the new growth area for digital fraud, with cybercrime surging 400% since 2021 according to MHA data. States like Bihar, Jharkhand, Uttar Pradesh, and Odisha report the highest growth.[94] Adding to this, India has approximately 400 million feature phone users for whom UPI's standard smartphone interface is inaccessible, and initiatives like UPI 123PAY, launched for feature phones, supports only limited languages and requires numeric literacy that first time users often lack. MicroSave Consulting found that these users require some assistance and cannot independently complete digital payment processes.[95]

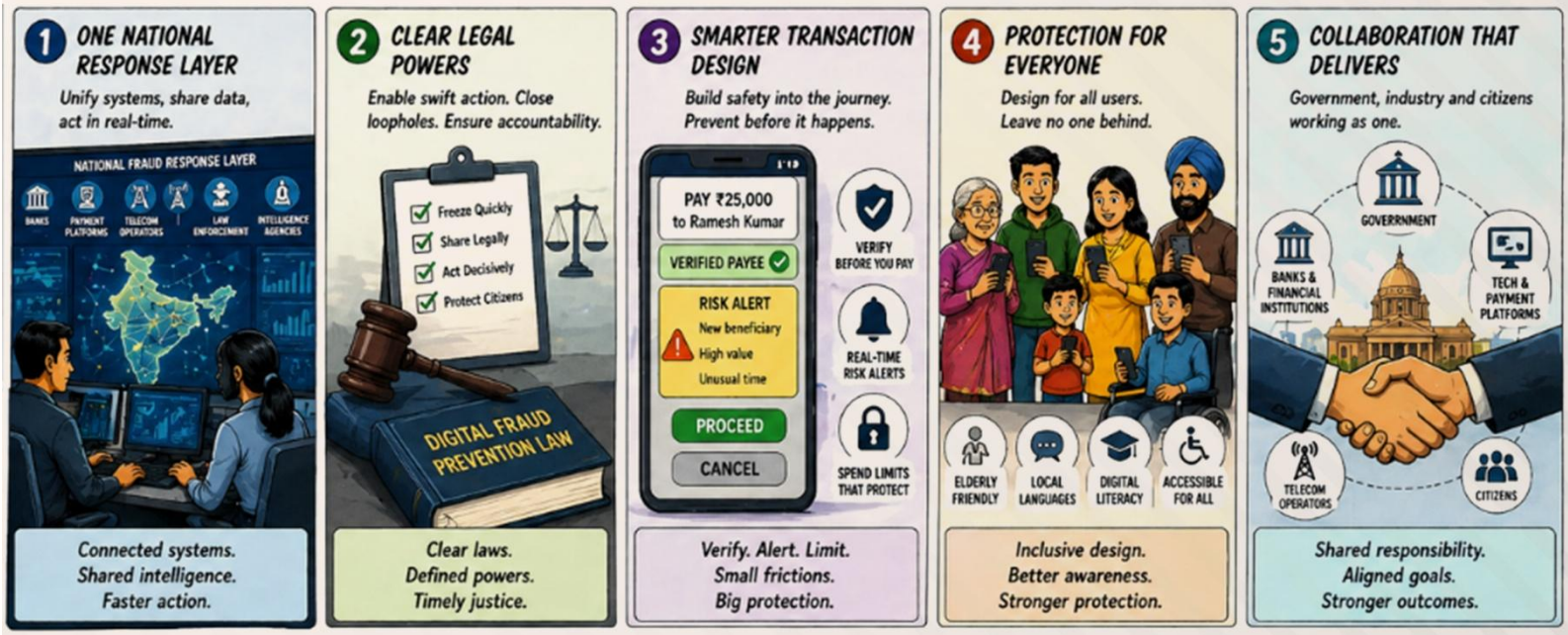
The language gap further widens the vulnerability. Fraudsters exploit this gap, using local dialects and familiar social references to build trust, while the security warnings in English fail to convey urgency. The NCRP claims multilingual support but plans for comprehensive regional language coverage remain incomplete. Similarly, UPI 123PAY covers only 7 of India's 22 scheduled languages.

For persons with disabilities, the gaps are structural. A 2024 usability evaluation of major UPI apps with 15 visually impaired participants found buttons without clear labels, hidden menus for critical actions like PIN resets, and no audio alerts when transactions succeed or fail. At the same time, there has been a movement towards making the digital realm more accessible.[96] The Supreme Court in *Pragya Prasun v. Union of India* in April 2025 ruled that digital access is a fundamental right and mandated alternative KYC methods for persons with disabilities.[97] In addition, the RBI's October 2024 circular requires all payment system participants to comply with IS 17802 accessibility standards, but implementation is still unfolding.[98]

As we delve deeper into the AI era, a new concern that has propped up is that AI fraud detection may itself create new forms of exclusion. Models trained on urban, digitally mature transaction patterns risk flagging legitimate transactions by rural users, new digital users, or users with irregular patterns as suspicious. The RBI's FREE-AI framework mandates that AI models be free from discriminatory bias and explainable, but operationalising this requirement across India's diverse user base, where only 20% have received any cyber safety training, remains among the most difficult design challenges in the digital payments ecosystem.

[93] Aayat, A. (2025). Cyber fraud costs Goa over ₹74 crore in three years. The420.in. https://the420.in/goa-cyber-fraud-74-crore-losses-seniors-2023-2025/
[94] Awasthi, S. (2025, October 28). Digital deception in rural India and the AI counter-offensive. Observer Research Foundation. https://www.orfonline.org/expert-speak/digital-deception-in-rural-india-and-the-ai-counter-offensive
[95] Lonkar, P., Menon, S., & Pathak, A. (2023, October 10). UPI 123Pay: The four-leaf clover for feature phone-based payments in India? Microsave. https://www.microsave.net/2023/10/10/upi-123pay-the-four-leaf-clover-for-feature-phone-based-payments-in-india/
[96] Rajput, M. S., & Thakur, Y. S. (2024). Bridging the visual gap: Usability evaluation of UPI smartphone apps for users with visual impairments. International Journal of Social Sciences and Management Review, 8(3). https://ijssmr.org/vol-8-issue-3/bridging-the-visual-gap-usability-evaluation-of-upi-smartphone-apps-for-users-with-visual-impairments/
[97] Supreme Court of India. (2025, April 30). Pragya Prasun & Ors. v. Union of India & Ors. Writ Petition (Civil) No. 289 of 2024. https://indiankanoon.org/doc/68332080/
[98] Reserve Bank of India. (2024, October 11). Facilitating accessibility to digital payment systems for persons with disabilities – Guidelines (RBI/2024-25/83, CO.DPSS.POLC.No.S-708/02-12-004/2024-25). https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12741&Mode=0

4.
Policy Recommendations



India's digital payment infrastructure has achieved remarkable scale, but the fraud ecosystem has expanded alongside it. The preceding sections of this report trace how psychological manipulation, access to telecom infrastructure, and cross-border coordination have led to significant financial losses. At the same time, although institutional responses are expanding, structural fragmentation and resource constraints continue to limit the effective enforcement of safeguards against these scams.

The recommendations that follow do not propose an entirely new structure. India already has key building blocks, including the 1930 helpline, and the Citizen Financial Cyber Fraud Reporting and Management System, MuleHunter.AI, the FRI, the DPIP, and regulatory guidance from the RBI. The primary need is consolidation. Accordingly, this section argues that these components must be integrated into a common governance and operational framework, backed by enforceable timelines, clear legal authority, and design choices that reflect the diversity of India's digital payment users.

4.1 Building a National Fraud Intelligence and Response Layer

India's digital payments fraud architecture has expanded rapidly, but its institutional design remains fragmented. Reporting systems, telecom-side indicators, and emerging intelligence platforms now coexist within the broader response framework. Yet these mechanisms do not function as a unified national layer capable of converting fraud signals into fast, standardised action. As a result, the system generates information across multiple points, but responses remain uneven and often depend on the operational capacity of individual institutions rather than the strength of the system as a whole.

The next stage of reform should focus on consolidation. A national fraud intelligence and response layer must bring all major actors into a common operational chain, including banks, NBFCs, UPI participants, payment aggregators, wallets, telecom operators, and law enforcement agencies. As noted earlier, fraud networks exploit institutional gaps. A response system that does not bind the ecosystem together through mandatory participation will continue to leave space for rapid fund movement across disconnected channels.

At present, fraud victims must navigate multiple institutional pathways. This fragmentation limits the system's ability to track a case from the first complaint to final action. A national response layer should therefore rest on a shared case architecture that assigns a common identity to each fraud event across systems. This would strengthen accountability by making it easier to identify where delays occur and whether prevention mechanisms translate into recovery for victims.

More broadly, fragmentation weakens both enforcement and recovery because no single institution has a complete view of the case trajectory, from first report to fund freeze, onward tracing, investigation, defreeze, and restitution. A unified fraud intelligence and response layer should enable intelligence to move with the case rather than remain confined within institution-specific silos. It would also shift performance measurement beyond narrow prevention metrics toward end-to-end outcomes, including the actual restoration of funds to victims.

This architecture must also operate under binding response standards. Digital payment fraud unfolds within minutes, but institutional action often relies on delayed escalation or uneven integration. A credible national layer should therefore impose time-bound obligations for complaint acknowledgement, provisional freeze action, inter-institutional alert transmission, review of flagged accounts, and decisions on defreeze and restitution. Without enforceable timelines, the response chain will remain slower than the fraud it is meant to contain.

A stronger national layer must also enable transaction-level intelligence integration. Banks can detect transaction anomalies, telecom providers can flag suspicious communications, and law enforcement agencies hold complaint data. At present, however, these intelligence streams remain only partially connected which means interventions often occur only after funds begin to move. A more effective architecture should integrate telecom-side risk signals with transaction anomalies before payment execution or immediately at the point of transfer.

Finally, the national response layer must be supported by a common governance framework for fraud intelligence. At present, the core challenge lies in the reliability and operational value of available data. Mule accounts are often short-lived, and delayed flagging reduces their preventive value while also exposing innocent recipients to unnecessary account restrictions. Fraud intelligence should therefore operate under common standards for validation, confidence levels, and accountability for action taken on the basis of alerts. The DPIP can play a critical role in this architecture by integrating banking, telecom, and complaint-based signals into pre-transaction alerts. However, its effectiveness will depend on the presence of a robust and shared governance framework.

4.2 Legal and Regulatory Reforms

India's response to digital payment fraud is increasingly constrained by legal and regulatory limits. The framework governing fraud prevention, freezing, data sharing, redress, and prosecution has not evolved at the same pace as the ecosystem itself.

Different countries have adopted different approaches to regulate digital payments and fintech. In the United States, for instance, the emergence of Society for Worldwide Interbank Financial Telecommunication (SWIFT) in the late 1970s marked a major shift by offering a secure and convenient platform for online money transfers. Over time, fintech growth in the U.S. has been driven by digital payments and blockchain technologies. However, this rapid expansion has also introduced challenges, including regulatory uncertainty, privacy and cybersecurity concerns, and unequal access to technology among low-income groups.[99] To address these issues, multiple regulators, including the Consumer Financial Protection Bureau (CFPB), the Office of the Comptroller of the Currency (OCC), and the U.S. Securities and Exchange Commission (SEC), have introduced measures to strengthen consumer protection and financial stability. A key development was the Electronic Signatures in Global and National Commerce Act (ESIGN Act), which granted legal recognition to electronic signatures and contracts, thereby supporting the growth of digital payments and credit systems. At the state level, money transfer regulations have evolved unevenly, with jurisdictions such as California adopting early frameworks and New York developing more recent approaches. At the global level, institutions like the Financial Stability Board (FSB) emphasise the need to balance innovation with risk management. Overall, the U.S. fintech regulatory landscape remains dynamic, with regulators increasingly adopting a more coordinated and collaborative approach to promote innovation while safeguarding consumers and the financial system.[100]

In the United Kingdom, the regulatory framework is primarily governed by the Financial Conduct Authority (FCA), along with key legislations such as the Financial Services and Markets Act 2000, E-Money Regulations 2011, and the Payment Services Regulations 2017, which aim to ensure consumer

[99] Baldwin, Richard, and Beatrice Weder di Mauro. 2019. Economics in the Time of COVID-19.
[100] Financial Stability Board. 2019. FSB Report Assesses FinTech Developments and Potential Financial Stability Implications. Press Release

protection and efficient payment systems. At the European level, the Revised Payment Services Directive (PSD2) promotes open banking and data sharing. While India adopts a system-centric regulatory model through UPI, the UK follows an entity-centric approach that relies on licensing, an open banking framework, and strong consumer protection norms to regulate digital payment. These developments reflect a balanced approach that encourages fintech innovation while maintaining robust regulatory oversight and consumer protection.

India's response to digital payment fraud is increasingly constrained by legal and regulatory limits. The framework governing fraud prevention, freezing, data sharing, redress, and prosecution has not evolved at the same pace. At present, the Indian regulatory landscape remains fragmented. Banking regulations govern the activities of banks and other financial institutions, prescribing capital requirements, risk management practices, lending norms, and consumer protection mechanisms.[101] At the same time, the government has launched initiatives to promote digital payments and strengthen the Fintech ecosystem. The RBI has established a regulatory sandbox that allows fintech firms to test innovative products and services in a controlled environment.[102] It has also introduced rules for digital payments, including two-factor authentication for mobile banking and regulations on prepaid payment instruments for mobile wallets. Regulatory measures such as KYC requirements and transaction limits aim to prevent fraud and misuse, while payment aggregators must obtain authorisation and comply with prescribed standards. Fintech providers are required to adhere to security norms and maintain transaction records. The RBI has also issued guidelines for online lending platforms that emphasise transparent pricing and customer privacy.[103] Securities regulations address the issuance, trading, and sale of financial instruments such as stocks, bonds, and derivatives, with the objective of protecting investors and ensuring fair and transparent markets.[104] Consumer protection regulations require financial institutions to treat customers fairly through clear disclosures, safeguards against unfair or deceptive practices, and grievance redress mechanisms.[105] Payment regulations govern electronic payments, money transfers, and remittances, ensuring system security, and compliance with Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) requirements.[106] Data protection frameworks further regulate the collection, use, and security of customer data held by financial institutions.[107]

However, a key concern is whether the current regulatory framework is keeping pace with rapid technological change. As financial services become increasingly digital, risks such as cyber fraud and data breaches are rising.[108]Yet India continues to rely largely on traditional laws such as the Bharatiya Nyaya Sanhita (BNS) 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), alongside the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023.

With the enactment of the BNS, the criminal law framework for addressing digital fraud has been updated. Section 318 of the BNS defines cheating broadly, covering acts of deception that induce a

---

[101] Nayak, R. 2021. Banking regulations: Do they matter for performance? *Journal of Banking Regulation* 22: 261–74
[102] Reserve Bank of India. 2024. Enabling Framework for Regulatory Sandbox. Available online: https://fintech.rbi.org.in/FS_Publications?id=1262
[103] ETtech. 2022. All Digital Loans Have to Comply with New Norms by Nov 30: RBI. The Economic Times. Available online: https://economictimes.indiatimes.com/tech/technology/ensure-existing-loans-comply-with-new-rules-by-nov-30-rbi-tells-digital-lenders/articleshow/93952962.cms
[104] Christensen, Hans B., Luzi Hail, and Christian Leuz. 2016. Capital-Market Effects of Securities Regulation: Prior Conditions, Implementation, and Enforcement. *The Review of Financial Studies* 29: 2885–924
[105] Chawla, Neelam, and Basanta Kumar. 2022. E-Commerce and Consumer Protection in India: The Emerging Trend. *Journal of Business Ethics* 180: 581–604.
[106] Pramani, Rahul, and S. Veena Iyer. 2023. Adoption of payments banks: A grounded theory approach. *Journal of Financial Services Marketing* 28: 43–57.
[107] Kost, Edward. 2023. Top 8 Cybersecurity Regulations for Financial Services.
[108] Sarkar, Bikramjit, Abhirup Mukherjee, Arundhati Ghosh, Chirag Chakraborty, R. Kiruthiga, Kanhaiya Kumar, and Debashis Barman. 2023. An investigation of different types of cyber-attacks and their detection and prevention. *AIP Conference Proceedings* 2878: 020015.

person to deliver property or suffer loss. This provision is wide enough to include online frauds, for instance, where a fraudster sends a fake UPI collect request or uses a deceptive chatbot to trick users into authorising payments. The BNS also includes provisions on organised crime and cyber offences, which apply when coordinated groups or syndicates carry out fintech fraud. Importantly, it retains strong extraterritorial jurisdiction, allowing Indian authorities to prosecute offences committed outside India if they target individuals or computer systems within India. This is particularly relevant for cross-border phishing and digital asset-based frauds. However, fintech-related crimes often move faster than traditional legal processes, making it critical that digital evidence, such as transaction logs, electronic records, and device data, is not rejected on technical grounds. With the transition from the Indian Evidence Act, 1872 to the BSA, the core principle underlying the earlier Section 65B certification has been retained. At the same time, a close reading of the new law suggests potential internal inconsistencies. On one hand, it places electronic records on par with documentary evidence; on the other, it prescribes a separate procedure for their admissibility. This may reopen interpretative debates that were considered settled by the Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal decision. The Adhiniyam also expands the scope of electronic and digital records and clarifies that data obtained from communication devices or cloud systems can be treated as valid documents, subject to prescribed legal conditions.[109] Fintech fraud cases frequently rely on such evidence, including UPI transaction logs, payment aggregator settlement records, and device-capture videos recorded under Section 105 of the BNSS. It is therefore essential that rules on the admissibility of such evidence align clearly with procedural law.

Jurisdictional issues are partly addressed by Section 4(5)(c) of the BNS, which extends Indian penal jurisdiction to persons located outside India if they target computer resources within India. This enables the prosecution of cross-border offences such as phishing, SIM swap frauds, and virtual digital asset (VDA)-based scams. However, in the absence of clear SoPs and adequate technical training for investigators and other stakeholders, the effective application of these provisions may remain challenging.

Other legislative instruments, such as the 2008 amendments to the Information Technology Act 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended subsequently in 2022, 2023, and 2025) provide an important legal basis for addressing cyber fraud. These frameworks criminalise offences such as identity theft[110] and cheating by personation,[111] enable compensation for privacy breaches, and grant safe harbour protection[112] to intermediaries that comply with due diligence requirements. They also empower CERT-In to issue directions relating to incident reporting, time synchronisation, data retention, and KYC obligations for virtual asset service providers operating in India.

These provisions are directly relevant to common digital payment frauds, including the creation of fake UPI IDs, misuse of OTPs or passwords, and impersonation of bank officials to induce payments. In addition, Section 43A introduces a civil liability mechanism by holding companies accountable for negligence in maintaining reasonable security practices when handling sensitive personal data, thereby requiring them to compensate affected individuals. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, read with the 28 October 2022 and 6 April 2023 amendments, require intermediaries to publish terms of use, take down unlawful content upon actual knowledge, appoint grievance officers in India, comply with orders of the Grievance Appellate Committee, and understand measures such as down-ranking or user identification in cases involving misinformation or deepfakes. Fintech platforms that operate as intermediaries for payment information,

[109] Sk. Shireen, "Electronic Evidence", available at: https:/ /cdnbbsr.s3waas.gov.in/ s3ec01a0ba2648acd23dc7a5829968ce53/uploads/ 2024/12/2024122766.pdf
[110] Section 66C of Information Technology Act, 2000
[111] Section 66D of Information Technology Act, 2000
[112] Section 79 of Information Technology Act, 2000

peer-to-peer payment requests, or wallet accounts must therefore demonstrate due diligence to retain safe harbour protections. Further, the CERT-In directions issued on April 28, 2022 under Section 70B(6) of the Information Technology Act 2000 introduced a six-hour reporting window for specified cyber incidents, mandatory log retention for 180 days, and synchronisation with Indian time sources. These requirements bring payment gateways, wallets, UPI apps, and even offshore exchanges offering services in India within their ambit. More recently, amendments by the MeitY in 2025 to Rule 3(1)(d) have further tightened due diligence obligations for intermediaries to address synthetic media and deepfake-based fraud, a category that increasingly overlaps with KYC spoofing in fintech apps.[113]

Under the Digital Personal Data Protection Act 2023, banks and similar entities are classified as "data fiduciaries." Fintech companies that collect personal and financial data, such as names, addresses, masked Aadhaar details, PAN, bank account information, device identifiers, location data, and behavioural patterns, to provide services like loans, wallets, prepaid instruments, or digital payments also fall within this category. These entities must obtain valid consent through clear notice, process data only for specified purposes, ensure data accuracy, implement reasonable security safeguards, report data breaches to the Data Protection Board and affected individuals, and delete data once it is no longer necessary unless retention is mandated by law.

However, certain practical challenges remain. The consent framework envisioned under the Act, particularly in enabling informed and granular user choice, is still evolving. In practice, users often encounter broad "accept all" options rather than meaningful control. In addition, the establishment of a fully functional Data Protection Board is still underway.

At the same time, unlawful disclosure of personal financial data to third-party advertisers or recovery agents would constitute a breach. Where such disclosure leads to identity theft or unauthorised transactions, liability would arise not only under the penalty provisions of the Digital Personal Data Protection (DPDP) Act, 2023 but also under Section 43A of the IT Act, 2000. As the 2025 draft rules emphasise processor accountability and cross-border data transfer conditions, fintech entities that rely on foreign cloud or SaaS services must execute DPDP-compliant contracts and ensure that CERT-In reporting requirements align with breach notification obligations under the DPDP framework.[114]

The IT Act 2000 and the DPDP ACT 2023 primarily address AI-related risks only when they result in a security or personal data breach. Issues such as performance degradation, algorithmic bias, or service manipulation remain largely outside their scope. While these laws are robust for their original purposes, they were not designed to address the distinct risks arising from AI systems.

India's response to digital payment fraud is therefore increasingly constrained by legal and regulatory limits. As a result, institutions can often identify suspicious activity without a sufficiently clear or timely legal basis to intervene, while victims may report fraud promptly but do not receive equally swift resolution or procedural clarity.

The key priority should be to establish a clear legal basis for short-duration protective restraint in cases of suspected digital payment fraud. At present, the law does not adequately bridge the gap between identifying a suspected mule account or fraudulent credit and imposing an immediate, reviewable hold before funds are transferred or withdrawn. Existing attachment and seizure powers are designed for formal investigation and adjudication, not for the speed at which digital fraud now occurs. This creates a critical gap in the early stages of a fraud event, when rapid intervention is most effective. The legal framework should therefore allow regulated entities to impose narrowly tailored, time-bound protective

[113] Aabha Singh & Ranjana Sharma, *Fintech Crimes and Indian Legal Responses: A Critical Examination*, 13(11) International Journal of Creative Research Thoughts u165 (2025)
[114] The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

holds on funds or accounts flagged through approved fraud detection systems, subject to strict reporting, oversight, and review mechanisms.

Second, as highlighted earlier in this report, it is important to establish an explicit legal basis for cross-institutional fraud intelligence sharing. The Digital Personal Data Protection Act 2023 permits data processing for the prevention, detection, investigation, or prosecution of offences. Government-led mechanisms such as the Citizen Financial Cyber Fraud Reporting and Management System and the DIP etc. also support this objective. However, these arrangements do not constitute a comprehensive framework for continuous fraud intelligence sharing across banks, payment service providers, telecom operators, and public agencies. The law does not clearly define the full scope of proactive data sharing for fraud prevention, the categories of data that may be exchanged, or the accountability and review standards that should apply when institutions act on shared intelligence.

Criminal procedure for cross-jurisdictional digital fraud also requires reform. The current framework remains only partially aligned and often involves numerous low-value transactions. Cybercrime complaints reported through the NCRB are handled by the relevant State or Union Territory law enforcement agencies, while the e-Zero FIR pilot introduced in 2025 applies only to cyber financial fraud complaints above ₹ 10 lakh. A stronger framework should enable seamless cross-jurisdictional registration and handling of digital payment fraud complaints. The threshold for the e-Zero FIR mechanism should be lowered to include frauds below ₹ 10 lakh, ensuring broader coverage. This expansion should explicitly include both UPI-based and non-UPI digital payment frauds, making the protection rail-agnostic.

Ultimately, India requires a techno-legal solution that embeds privacy by design, ensuring that fraud prevention mechanisms operate effectively while safeguarding user rights and data protection principles.

4.3 Redesigning Transaction Flows for User Protection

India's digital payments architecture has prioritised speed and ease of use. While this design has driven adoption, it has also created transaction flows in which users can be manipulated into authorising fraudulent payments before the system or a third party can intervene.

The NPCI already operates a risk policy framework for UPI. This includes daily transaction caps of ₹ 1 lakh for person-to-person transfers, a limit of 20 outgoing transactions per day, real-time risk scoring, device and SIM binding, and a four-hour cooling-off period that restricts new device registrations to ₹ 5,000 for the first 24 hours. These are meaningful safeguards that have strengthened the ecosystem. The recommendations in this section do not seek to replace this framework but to extend it in areas where the current design still leaves structural vulnerabilities, particularly in high-value transfers to unfamiliar recipients.

The most consequential remaining gap is the absence of a fully interactive confirmation of Payee system that operates across all retail payment rails, with standardised match responses and warning flows. As noted earlier, the RBI, through its circular dated 30 December 2024 has already mandated a beneficiary bank account name look-up facility for RTGS and NEFT, to be implemented by all participating banks by 1 April 2025.

Building on this foundation, the RBI can evolve the existing name look-up facility into a comprehensive Confirmation of Payee system across UPI, IMPS, RTGS, and NEFT. As discussed in Section 3.6, this should

include a graduated four-state response: a full match, a close match that returns the actual account holder name to the payer, an explicit no-match warning, and an unavailable outcome. This should be accompanied by a standardised warning flow and a clear cancellation option at the point of payment. The NPCI and payment service providers should be required to build a real-time name-matching application programming interface that flags discrepancies to users before execution The RBI should also publish compliance metrics to ensure transparency and accountability across the ecosystem. For reference, the United Kingdom's system has processed over two billion checks by March 2024 and achieved approximately 99 per cent coverage of Faster Payments transactions, demonstrating the scale and effectiveness that a fully implemented, scheme-level system can achieve.[115]

The second intervention concerns risk calibrated delays for transfers to unfamiliar recipients. While the existing daily cap of ₹1 lakh and the 20 transaction limit provide a ceiling, they do not differentiate between a transfer to a payee with whom the sender has a transaction history and a transfer to a completely new recipient. RBI should mandate tiered cooling off periods for UPI person to person transfers that exceed defined thresholds when directed to first time recipients. Additionally, the lag should be calibrated to the payer to payee relationship rather than applied uniformly, so that first time recipients attract a longer review window while established payees pass through with minimal friction.

Adding to the above, as established in Section 3, scam scripts are engineered to isolate victims from external reality. In many documented cases, the most effective disruption has been a phone call from a trusted contact. Payment platforms should therefore allow users to register one or two trusted contacts who receive an automated alert whenever a high value transfer to a new recipient is initiated. The alert would not require approval to proceed but would introduce a social checkpoint that disrupts the scammer's isolation strategy. This feature should be opt-in but actively promoted during onboarding and through periodic prompts within UPI apps, with simplified activation for senior citizens and users identified as high risk through behavioural profiling.

Authentication reforms should complement these transaction flow changes. The RBI's Authentication Mechanisms for Digital Payment Transactions Directions, issued in September 2025, require all domestic digital payments to adopt two-factor authentication by April 1, 2026, with at least one dynamic factor for non-card present transactions.[116] This shift toward device-bound passkeys and biometric verification is necessary modernisation. Payment system providers should implement adaptive authentication that triggers additional verification, such as biometric confirmation or a call-back to the registered mobile number, when a transaction is flagged by the FRI or when the payment pattern deviates from the user's established baseline. The RBI's suggestion to use DigiLocker as a notification and confirmation platform for high-risk transactions should be operationalised as a formal requirement rather than left as a discretionary option for issuers.

The RBI discussion paper on Safeguards (cited above), also proposes customer induced controls at an account level, more importantly, a switch on/off facility for individual digital payments modes and a master kill switch to disable all payment channels at once, drawing from the precedents set in Singapore and Australia. This report supports the same.

Finally, the irrevocability of UPI transactions requires a structured recourse mechanism. Unlike credit card systems that offer chargeback windows of 30 to 120 days, UPI settlements are instant and can be reversed only with the beneficiary bank's cooperation, often impossible when the beneficiary is a mule account. The RBI's draft compensation scheme of March 2026, which proposes coverage of 85% of net

[115] Payment Systems Regulator. (2022, October). Extending Confirmation of Payee coverage: Response to consultation CP22/2 (PS22/3). https://www.psr.org.uk/media/migeob4s/ps22-3-extending-cop-coverage-oct-2022.pdf
[116] Reserve Bank of India. (2025, September 25). Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025 (RBI/2025-26/79; CO.DPSS.POLC No. S-668/02-14-015/2025-2026). https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12898&Mode=0

loss or ₹ 25,000 for small-value fraud cases, acknowledges this structural gap. This scheme should be finalised and expanded in scope. In parallel, the NPCI should explore a conditional hold mechanism for flagged transactions. Under such a system, payments to accounts identified as high risk through the Suspect Registry or FRI could be held in escrow for a defined window before settlement. This would introduce a reversibility layer that does not currently exist and reduce the burden on victims to recover funds after they have already entered the mule laundering chain.

4.4 Accessibility and Inclusive Design in Fraud Safeguards

As Section 3.6.1 highlighted, the populations most vulnerable to fraud are often those least served by existing safeguards.

The first priority is to strengthen multilingual fraud warnings and reporting infrastructure. UPI 123PAY, the feature phone interface for UPI, currently supports only 7 of India's 22 scheduled languages and often requires a level of numeric literacy that first-time users may not possess. Similarly, the NCRP's efforts to provide comprehensive regional language coverage remain incomplete. At the same time, there is a clear opportunity to build on existing progress. The NPCI has already partnered with the Bhashini platform to enable conversational payments in Indian languages. As of May 2025, Bhashini supports over 35 languages and integrates more than 1,600 AI models across platforms, including NPCI's Interactive Voice Response (IVR) systems. This capability should be extended to fraud warning interfaces within UPI apps to ensure that risk communication is accessible and actionable.[117]

Age-specific protections also require prioritisation. Senior citizens are disproportionately targeted, as "digital arrest" scams exploit high levels of trust in authority and limited familiarity with digital interfaces. Payment platforms should therefore offer a "senior safe mode," activated either through self-selection at onboarding or through age identification based on KYC records. This mode would include lower transaction limits for new recipients, mandatory cooling-off periods for transfers above a defined threshold, automatic alerts to trusted contacts, and simplified, high-contrast interfaces with larger text. The RBI, in its discussion paper on safeguards (ibid), has also proposed an additional authentication layer, an authorisation process involving a trusted person for high-value transactions, particularly for individuals aged 70 and above and for persons with disabilities.

Banks should be required to flag accounts held by individuals above the age of 60 for enhanced monitoring under the FRI framework, with any high-risk signal triggering a call-back to the registered mobile number before the transaction proceeds.

Building upon this, accessibility for persons with disabilities must also be prioritised. A 2024 usability evaluation of major UPI apps cited above, also found issues such as buttons without clear labels, hidden menus for critical actions like PIN resets, and the absence of audio alerts for transaction outcomes. In line with binding directions of the Supreme Court of India, UPI apps and banking platforms must ensure screen reader compatibility across all transaction flows, provide audio confirmations at every stage of a payment, including pre-transaction warnings, and support alternative authentication methods such as voice-based or thumb-impression verification. The RBI should establish a compliance audit process for IS 17802 accessibility standards that mandates testing with persons with disabilities as evaluators, rather

[117] Inc42. (n.d.). NPCI to integrate AI-powered Bhashini to offer conversational payments in 22 languages. Inc42. https://inc42.com/buzz/npci-to-integrate-ai-powered-bhashini-to-offer-conversational-payments-in-22-languages/

than relying solely on self-certification by payment system participants. In addition, the NPCI should publish an annual accessibility compliance report covering all UPI member apps.

Lastly, as AI-driven fraud detection systems scale across Indian banking, models trained on urban, digitally mature transaction patterns risk flagging legitimate transactions from rural users, new digital users, and individuals with irregular payment behaviour as suspicious. The RBI's FREE-AI requires that such models remain free from discriminatory bias and are explainable. However, operationalising these principles demands concrete measures. Banks deploying AI-based fraud detection should be required to conduct and publish demographic impact assessments that measure false-positive rates across user segments defined by geography, age, income tier, and digital tenure. Where disparities exceed a defined threshold, institutions should retrain the model or recalibrate decision boundaries before continued deployment. Similarly, the DPIP, currently in its early stages, should embed fairness metrics as a core component of its AI governance architecture from the outset, rather than treating inclusion as an afterthought once the system becomes operational.

4.5 Strengthening Public Private Partnerships in Fraud Prevention

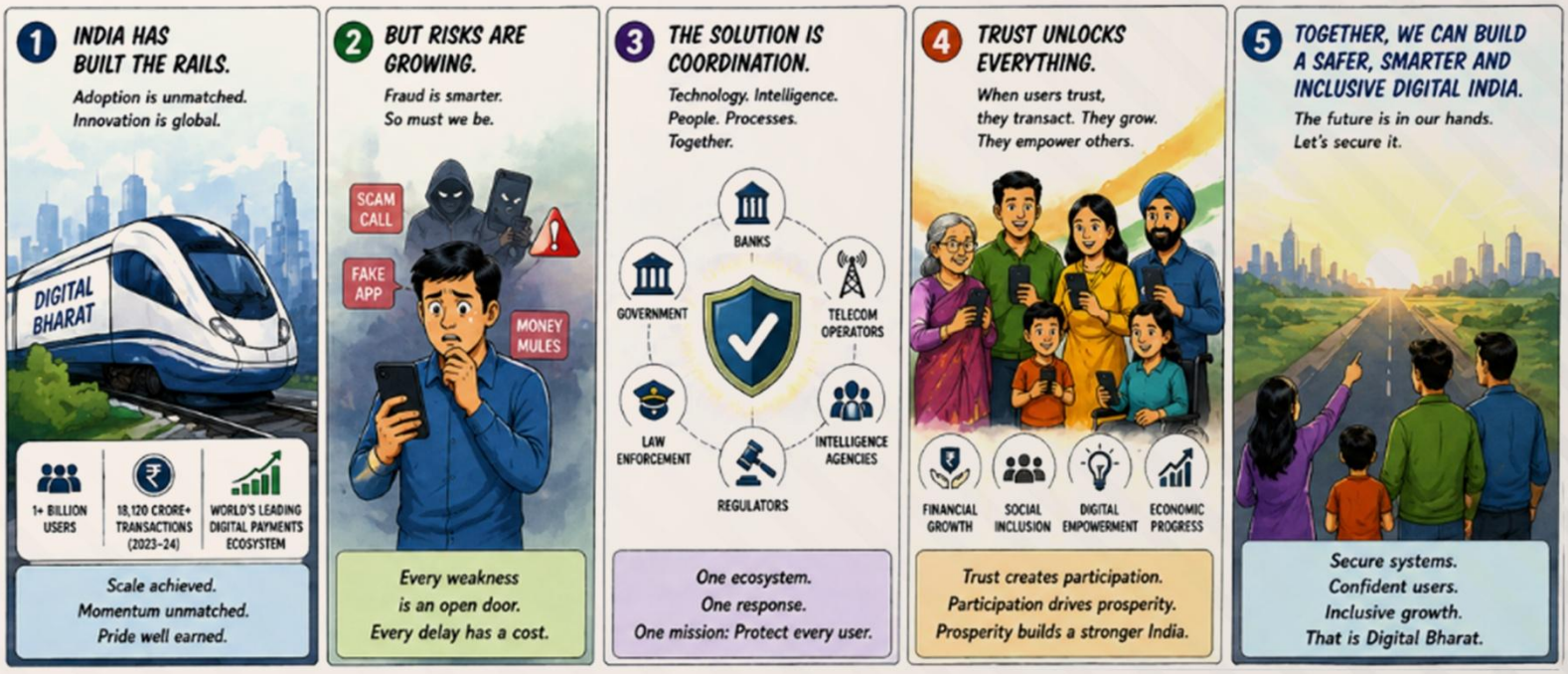
As mentioned in Section 2.4.2, the MoU which facilitated a PPP on cybersecurity incident response, capacity building, sharing of cyber threat intelligence specific to the financial sector, and advanced malware analysis, connects the operational visibility of a global payment network, such as its view of card testing patterns, digital skimming campaigns, and merchant level compromises, directly to the national incident response agency that coordinates cybersecurity action across Indian institutions.

The above agreement illustrates where the next stage of reform must focus. Global payment networks, cybersecurity firms, and threat intelligence providers possess operational visibility into card testing patterns, malware ecosystems, and compromised credential markets at a scale that no domestic agency can replicate. This is largely because the relevant data is generated from transaction flows and threat surfaces that lie outside the Indian banking perimeter. A structured and continuous public-private layer that taps into this visibility can therefore help close gaps that purely domestic mechanisms cannot address on their own.

Accordingly, this model should be extended in three directions. First, other national agencies, such as the I4C, the Reserve Bank Innovation Hub, and the Digital Intelligence Unit of the Department of Telecommunications, should be enabled to enter into comparable arrangements with other major payment networks and cybersecurity firms, with a clearly defined scope on the categories of data shared, the cadence of exchange, and the obligations of each side. Second, the intelligence generated through these partnerships should feed into the DPIP and the Suspect Registry, so that signals from global networks sit alongside domestic banking, telecom, and complaint data inside a common analytical layer, instead of remaining trapped in bilateral channels. Third, the governance of this layer should include published reporting on training reach, capacity building activity, and the categories of intelligence exchanged, so that the public private component of India's fraud response architecture is visible, accountable, and open to assessment over time.

5.

Conclusion



India’s digital payments system has reached a stage where the trust embedded in its architecture matters more than its ambition. The figures presented in this report reflect this clearly. Rising complaint volumes, coupled with low recovery rates, point to the need for a coordinated strategy involving all stakeholders, from individual users to the highest institutional authorities overseeing India’s digital payment ecosystem. While the institutional architecture requires further refinement, its expansion across reporting helplines, telecom side risk indicators, mule account intelligence, and AI-driven detection tools underscores the government’s commitment to building a comprehensive security framework.

This report finds that India does not face a shortage of components, but a shortage of consolidation.The 1930 helpline, the Citizen Financial Cyber Fraud Reporting and Management System, the Suspect Registry, MuleHunter.AI and related initiatives together constitute a substantial response infrastructure. However, these components operate as parallel systems rather than as a unified national layer. As a result, intelligence generated at one point in the chain often does not translate into timely action at another. This creates a fragmented ecosystem where improvements in prevention do not necessarily translate into higher recovery rates, leaving outcomes dependent on the speed differential between fraud and response.

As outlined in Section 4, the path forward lies in integrating existing components within a common operational and governance framework. This must be supported by enforceable timelines, a clear legal basis for protective restraint and intelligence sharing, redesigned transaction flows that introduce friction at points of highest risk, and accessibility standards that reflect the diversity of India's digital payment users.

The RBI’s recent discussion paper on safeguards, its March 2026 compensation scheme, and the Payments Vision 2028 indicate that policy direction is broadly aligned with the diagnosis presented in this report. Consolidating extant initiatives under an overarching mechanism will go a long way in addressing one of the most pressing challenges of India’s digital economy.


A FUTURE THAT BELONGS TO EVERY INDIAN.
Every payment safe.
Every citizen empowered.
Every opportunity unlocked.
Every dream within reach.
TRUST KEEPS INDIA DIGITAL
SECURE SYSTEMS. CONFIDENT USERS. INCLUSIVE GROWTH.
UPI
Payment Successful
₹

Author

Raunaq Sharma

Senior Research Associate, The Dialogue

Raunaq Sharma is a public policy professional specialising in Artificial Intelligence, Data Privacy, and Content Moderation. As a former Senior Associate at Chase India, he led key campaigns on online age verification, content governance, and AI safety for leading technology firms. His prior roles at Carnegie India, PRS Legislative Research, and the Office of the Advisor to the Chief Minister of Delhi have further strengthened his policy research credentials.

Contributors

Aastha Tiwari

Assistant Professor of Law, Maharashtra National Law University (MNLU), Mumbai

Aastha Tiwari is an Assistant Professor of Law at Maharashtra National Law University (MNLU), Mumbai, and a doctoral candidate specialising in the socio-legal dimensions of cyber voyeurism through the lens of privacy law. Her research sits at the intersection of artificial intelligence, data protection, and technology-facilitated crimes against women and children, with a focus on constitutional frameworks and emerging digital harms.

She holds an LL.M. from the National Law Institute University, Bhopal. A DAAD Scholar, she has studied privacy law at the Berlin School of Economics and Law, bringing a valuable comparative dimension to her work. Aastha has authored papers in high-indexed peer-reviewed journals and edited volumes on artificial intelligence, privacy law, and cybercrime. As Faculty In-charge of the Centre for Information Communication Technology and Law (CICTL) at MNLU Mumbai, she leads research initiatives, national and international academic collaborations, and capacity-building programmes. She is also a visiting faculty at Central Academy for Police Training, Bhopal.

Soham Jagtap

Senior Research Associate, The Dialogue

Soham Jagtap is a Senior Research Associate, at The Dialogue, focusing on AI and data protection. Instead of e-commerce and fintech. He holds an LLM in Law and Technology from NUJS, where he graduated with the highest distinction in 2023. His research explores the intersection of law and technology, with work spanning AI ethics, fintech policy, and justice delivery through technology. At The Dialogue, Soham contributes to shaping policies that balance innovation and public interest through rigorous legal research and analysis.

Kriti Singh

Associate Director - Programmes and Operations, The Dialogue

Programmes and Operations at The Dialogue, oversees programme execution, stakeholder coordination, and overall delivery. With over eight years of experience across journalism, communications, and public policy, she leads key verticals including Fintech, emerging technologies and the Creator and Platform Economy. Her experience in managing multi-stakeholder engagements across government, industry, and media ensures both strategic alignment and timely execution.

Ranjeet Rane

Organisational Partner and Lead of Fintech & Sustainable Finance, The Dialogue

Ranjeet Rane is Partner at The Dialogue, where he leads the Fintech and Sustainable Finance verticals. A public policy professional with over 15 years experience in tech policy, fi nancial regulation, and digital innovation, he previously led policy research at RBIH and ReBIT. Ranjeet is a PhD scholar, amateur birder, and longtime advocate for responsible innovation in India's digital economy.