Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 6 Issue 1 (2026)

Bridging the Last Mile: The Battle Against UPI Fraud in Rural India A Case from Maharashtra

Prof. Dr. Nishikant Jha,

Research Guide and Head, Department of Bachelor of Accounting and Finance, Thakur College of Science and Commerce (Autonomous), Thakur Village, Kandivali (E), Mumbai – 400101, Maharashtra, India, Email: drnishikantjha@gmail.com

Mr. Sagar Uttam Shinde

(Corresponding Author) Research Scholar, Assistant Professor, Department of Commerce & Management, Vaidyanath College, Parli-Vaijnath, Dist. Beed, MS 431515, Email - prof.sagar4u@gmail.com

Dr. Prashant Nike,

Assistant Professor, UGC MMTTC, University of Mumbai. Maharashtra, India, Email: - prashant@hrdc.mu.ac.in

Abstract

India's rapid adoption of digital payments, led by the Unified Payment Interface, has changed transactions and widened financial inclusion, reaching remote areas. Yet this progress has coincided with a sharp rise in digital fraud that hurts first generation, low literacy users. This teaching case examines a composite event from Latur district in Maharashtra, where a sixty-eight-year-old farmer, Ramesh Pawar, loses Rs. 85,000 after a fake KYC message and struggles to obtain redress. The discussion is set against rising UPI fraud and Maharashtra's cybercrime burden, and it highlights gaps in early detection, frontline policing, banking procedures, and digital literacy.

Presented as a character driven narrative grounded in official statistics, the case follows the actions and constraints of key stakeholders, including the local police station, State Cyber Cell, a cooperative bank, NPCI, and civil society groups working on digital literacy. It invites reflection on systematic accountability, limits of user responsibility rhetoric, and design of safeguards and grievance systems suited to rural contexts. The case is intended for postgraduate courses in public policy, law, digital governance, and financial regulation, and for practitioners concerned with inclusive and trustworthy digital payments.

Keywords: Digital fraud, digital literacy, phishing, rural fintech risk intersect, grievance redressal mechanisms

1 INTRODUCTION

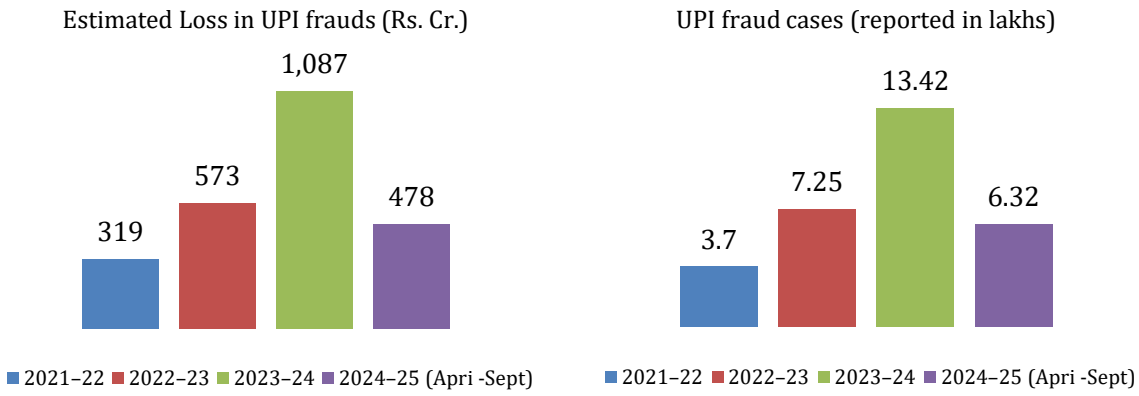
On a June evening in 2024, in a village in Latur, Maharashtra, a 68 year old farmer, Ramesh Pawar, sat outside his one room house with a keypad phone when a text arrived stating his KYC would expire and his UPI would be suspended unless he updated via a link. He had recently learned to use UPI to pay a supplier, recognized terms like KYC and RBI rules, and it seemed official. Lacking banking education or cyber safety training, he tapped the link, entered an Aadhaar linked number, and typed the OTP, believing he was following instructions. Within minutes, eighty-five thousand rupees saved for medical needs and farm inputs was debited. Shocked, he went to the cooperative bank branch, where staff, unsure how to handle UPI fraud, told him to visit the police station and call helplines.

At the police station, a junior officer dismissed the complaint as his own mistake, and an FIR was registered after three days, when his daughter and a self help group worker pressed for action. By that point, funds had passed through multiple mule accounts. When the case reached the Cyber Cell, investigators reconstructed the trail but were unable to recover money. The episode left him financially insecure and distressed, and wary of digital payments, amid rising UPI fraud and Maharashtra's cybercrime burden. His experience illustrates how a fraudulent message reveals failures in detection, frontline policing, banking procedures, and digital literacy across a fast growing fintech ecosystem.

2 DIGITAL INCLUSION AND DIGITAL RISK

Ramesh's experience reflects a broader pattern. India now processes over 10 billion UPI transactions each month, with UPI embedded in purchases from urban malls to rural mandis. Yet reported UPI related fraud has surged, exceeding

1.3 million incidents and more than ₹1,000 crore in reported losses in financial year 2023 to 2024 alone. Rural and semi urban users, often late adopters with limited digital literacy, are heavily represented within this rise.



Source: NPCI, Reserve Bank of India, GoI Cyber Reporting Portal

case study

In districts such as Latur, smartphone use has grown rapidly, yet structured digital safety education has not kept pace. Banking correspondents assist villagers in opening accounts and installing payment apps, but few sustained initiatives explain phishing, OTP misuse, or fraud reporting pathways in local languages. Meanwhile, cybercriminals deploy low cost bulk SMS tools, spoofed sender IDs, and localized scripts in Marathi or Hinglish to craft convincing alerts about KYC expiry or account suspension warnings.

The case raises three linked questions. How inclusive are digital financial safety nets for low literacy and elderly users? To what extent should institutions rather than individuals bear responsibility for fraud management, and which technical, institutional, and community-based features can protect first generation digital users effectively today?

3 KEY STAKEHOLDERS

3.1 Maharashtra State Cyber Cell and Latur Police

On paper, the Maharashtra State Cyber Cell is the apex authority for cybercrime in the state, offering technical support and investigative expertise. In practice, its resources are concentrated in major cities. Rural police stations, including in Latur, remain the first point of contact for victims yet often lack dedicated cyber personnel, digital evidence tools, or high speed connectivity.

In Ramesh's case, the Latur station treated the complaint as a routine banking issue rather than time critical digital theft. There was no dedicated terminal to log cyber complaints, no standard protocol for immediate escalation to the Cyber Cell, and limited awareness of online portals such as the National Cyber Crime Reporting Portal or the 1930 helpline. The delay proved critical, for by the time Cyber Cell officers in Aurangabad accessed the transaction logs, the funds had already passed through multiple intermediary accounts across states.

3.2 NPCI and the Banking System

NPCI manages the core infrastructure for UPI. It also operates risk scoring engines to identify suspicious transactions. However, many of these tools are calibrated around volume and pattern anomalies rather than the particular vulnerabilities of low-volume, rural users. Large, one-off transfers from such users may not always trigger additional checks.

Cooperative and regional rural banks, meanwhile, are often under-resourced. Branch managers have to balance traditional banking operations with new digital products but may lack specialized staff for fraud response. Freezing suspect transactions, escalating cases to higher-level fraud control teams, and guiding customers through grievance redressal processes are not yet embedded as standard operating procedures at the local level.

3.3 Civil Society and Digital Literacy Workers

NGOs and community-based organizations fill some of the awareness gaps. In Latur, a small NGO runs "safe digital" workshops using posters, flipbooks, and short talks at schools and self-help group meetings. It was an NGO worker who eventually encouraged Ramesh to insist on an FIR and to call 1930.

Yet these initiatives function on a narrow scale, rely on brief funding cycles, and are seldom embedded within state cybercrime strategies. Moreover, no formal channel exists by which such organizations can transmit aggregated field insights into policy design or enforcement priorities.

4 INDUSTRY AND REGULATORY CONTEXT

UPI is widely regarded as a flagship of public digital infrastructure. With interoperability, instant settlement, and zero merchant discount for many small firms, it has lowered entry barriers for millions of users and micro enterprises, aided by programs such as Jan Dhan Yojana and Aadhaar enabled authentication that laid basic rails for mass account ownership and identity verification.

Yet the same qualities that make UPI simple and ubiquitous also open attack surfaces, including fake KYC texts leading to phishing sites, links that push installation of remote access apps, and QR codes that entice users to receive money while in fact authorizing outbound payments, with syndicates industrializing these tactics by blasting thousands of messages each day and rapidly routing stolen funds through networks of mule accounts.

India's regulatory architecture offers consumer protection instruments: RBI norms on digital payment security and zero liability for unauthorized electronic transactions, alongside NPCI grievance mechanisms, are designed to safeguard customers who are not at fault; however, the persistent difficulty lies in ensuring effective implementation at the ground level.

- Rural bank branches may be unaware of or hesitant to invoke zero-liability provisions.
- Police stations often do not treat cyber fraud with the urgency given to physical theft, even though financial consequences may be comparable.
- Grievance portals and helpdesks use English and online systems, creating barriers for low literacy users.

Several Indian states have piloted more decentralized responses, including taluka level cyber volunteers and student cyber ambassadors, yet uptake remains uneven. In a high usage state such as Maharashtra, the distance between transaction growth and protective infrastructure is especially stark today.

5 CHARACTER SNAPSHOTS

To humanize the institutional analysis, the case employs composite character profiles that illuminate user vulnerabilities and system constraints through three figures.

5.1 Ramesh Pawar – Elderly First-time Digital User

Ramesh Pawar, an elderly first time digital user, stands in for millions of low income Indians encouraged to adopt UPI without sustained support for safe usage; his trust in anything that appears to come from the bank, willingness to share one time passwords when asked, and reluctance to challenge authority are shaped by age, social position, and limited exposure to formal institutions, and after the fraud he loses ₹85,000 and withdraws from digital payments altogether, undermining the financial inclusion aims that motivated UPI adoption.

5.2 Inspector Sunil More – Overstretched Station House Officer

Inspector Sunil More, an overstretched station house officer, leads a police station managing a wide range of traditional crimes with minimal staff; cyber complaints are viewed as technically complex and peripheral to core policing, so under high workloads and scant training he initially discourages a formal complaint and frames the incident as user negligence, and only persistent pressure from family and a civil society worker secures registration of an FIR and referral to the Cyber Cell.

5.3 Cyber Inspector Priya Kulkarni – Regional Cyber Specialist

Priya Kulkarni, a regional specialist based in the Aurangabad Cyber Cell, works with a small team that investigates cyber financial frauds across multiple districts; by analyzing transaction logs and bank data they trace the movement of the stolen funds through several mule accounts in different states, yet by the time the complaint reaches them balances are negligible, and she uses the case to argue for decentralized cyber desks and time bound FIR norms, insisting that digital crimes require digital speed responses.

6 PROBLEM DESCRIPTION

6.1 Timeline of Events

The core sequence unfolds across a few days. On day one, Ramesh receives a fake KYC text, follows the link, enters his credentials and an OTP, and loses ₹85,000. On day two, he visits his cooperative bank, and staff advise contacting police helplines but do not initiate account freezing. On day three, he approaches the local police station, the complaint is heard yet not formally recorded. On day four, after visits and NGO intervention, an FIR is registered and basic particulars are sent to the Cyber Cell. Between days five and fifteen, Cyber Cell investigators tracked the funds, only to find them scattered across mule accounts.

At each stage, vital opportunities slipped away. The bank ought to have flagged an unusually large transfer from a low activity account, and the police could have promptly registered and FIR and notified the Cyber Cell. Staff should have used helplines and portals on behalf of the victim rather than merely suggesting them.

6.2 Systemic Failures

The case reveals multiple structural weaknesses. First, delayed and reluctant FIR registration persists: hesitation among police to promptly record cybercrime complaints degrades evidentiary trails and suggests fraud is treated as less serious than theft of cash in many districts. Second, coordination is fragmented across banks, police, and the Cyber Cell; no standardized real time escalation protocol links actors, and each institution sees the problem through lenses of compliance, law and order, or technology, without integration. Third, rural centric fraud detection is limited, since current algorithms and heuristics are poorly calibrated to risk profiles of elderly and low volume users, for whom sudden large transfers should trigger extra checks or warnings. Fourth, digital literacy gaps and victim blaming persist: awareness efforts are intermittent, ill suited to local languages and usage patterns, and rarely evaluated for impact, and responsibility often shifts to the victim, who is blamed for clicking a link rather than seen as a client of a system that failed to protect him. Finally, psychosocial harms follow monetary loss, breeding shame, eroding trust in institutions, and prompting digital withdrawal, particularly among older users, undermining the long term success of financial inclusion policies.

7 WAYS FORWARD

This case examines how to design an inclusive and resilient antifraud architecture for rural UPI users and sets out three directions. First, strengthen frontline policing by mandating time bound cyber FIR norms requiring registration of cyber financial fraud complaints within twenty four hours, with compliance tracked through a state level dashboard; establish cyber desks at rural police stations with trained staff, internet, and direct channels to the State Cyber Cell; and integrate cybercrime modules into routine police training emphasizing victim centric handling, the importance of the golden hour, and collaboration with banks.

Second, redesign bank and NPCI protocols by requiring banks and payment service providers to build rural sensitive risk models that flag high value transfers from low activity accounts and trigger checks, such as a confirmation call or in app warning, before processing; operationalize standard operating procedures for rural branches to freeze suspect transactions and escalate cases to fraud control teams; and simplify and localize grievance redress interfaces using IVR and SMS in regional languages, missed call services, and assisted complaint filing through banking correspondents.

Third, scale and institutionalize digital literacy by developing a cadre of digital safety volunteers at gram panchayat level, similar to ASHA or Anganwadi workers, trained to explain basic cyber hygiene, helplines, and complaint procedures; embedding cyber safety content in community platforms such as SHG meetings, school assemblies, and agricultural extension sessions, using stories and role play rather than posters; and coordinating campaigns across

government, banks, NPCI, and civil society to deliver consistent messages, for example that no bank will ask you to share an OTP.

7.4 Rapid Scam Alert Systems

Use telecom networks and messaging platforms to broadcast time bound scam alerts in regional languages when fraud patterns are detected, for instance fake KYC or electricity bill messages, and encourage local banks, panchayats, and schools to reannounce these alerts in offline forums like markets and local community meetings; collectively, these measures redirect attention from blaming individual users toward building layered institutional safeguards adapted to rural realities.

8 DISCUSSION QUESTIONS

1. Who should bear primary responsibility for preventing cases like Ramesh's, namely the user, the bank, the regulator, NPCI, or the police? How can accountability be distributed without weakening it?
2. What compromises emerge between making UPI simple to use and adding stronger security checks, particularly for elderly or low literacy users?
3. If you were advising the Maharashtra government, which two or three reforms would you prioritize over next twelve to eighteen months to reduce rural UPI fraud?
4. How can NGOs and community organizations be systematically embedded in cybercrime prevention and response frameworks, rather than treated as ad hoc partners?
5. Are there examples from other Indian states or comparable countries that Maharashtra could adapt to its own context for rural digital safety?

9 TEACHING NOTE (FOR INSTRUCTORS)

This case is suitable for postgraduate courses in public policy, digital governance, financial regulation, and law, as well as executive training for regulators, law-enforcement personnel, and fintech practitioners. It can be used to achieve four learning objectives:

- Understand systemic challenges in rural cybercrime enforcement and digital financial protection.
- Analyse stakeholder incentives and constraints across government, industry, and civil society.
- Design context-sensitive policy and process interventions for inclusive digital safety.
- Reflect on ethical questions around victim blaming, consent, and trust in digital public infrastructure.

Suggested teaching flow:

1. **Narrative immersion:** Ask students to read Ramesh's story and identify points where different choices by any actor might have changed the outcome.
2. **Systems mapping:** In small groups, have participants draw the ecosystem of actors (user, bank, police, Cyber Cell, NPCI, NGOs, telecom operators) and map information and power flows among them.
3. **Policy lab:** Assign groups to represent different stakeholders and negotiate a shared action plan to reduce rural UPI fraud over a three-year horizon.
4. **Debrief:** Evaluate proposed solutions, identify implementation challenges, and relate them to wider debates on digital public infrastructure, inclusion, and risk.

References: -

Journal articles

1. Dam, L. B., & Deshpande, K. (2021). Unified payment interface (UPI) platform: Conniving tool for social engineering attack. *Pacific Business Review International, 14*(3), 17–28.

2. Gupta, S. (2025). Securing Unified Payments Interface: A deep learning approach for fraudulent transaction detection. *Journal of Global Research in Multidisciplinary Studies, 1*(11), 1–8. https://doi.org/10.5281/zenodo.17551619
3. Jagtap, S. S. (2024). Evaluating user perceptions and security concerns in Unified Payments Interface (UPI) services. *International Journal of Research Publication and Reviews, 5*(8), 2219–2223. https://doi.org/10.55248/gengpi.5.0824.2136
4. Kaur, S., Mishra, H., & Goyal, A. (2023). Cyber-security in UPI payments. *International Journal for Research in Applied Science and Engineering Technology, 11*(5), 4955–4958. https://doi.org/10.22214/ijraset.2023.52175
5. Kumar, J., & Rani, N. (2025). Optimized machine learning and deep learning approaches for effective detection of fraud in Unified Payments Interface (UPI) transactions. *International Journal on Science and Technology, 16*(4). https://doi.org/10.71097/IJSAT.v16.i4.9525
6. Mukhopadhyay, N., & Mukhopadhyay, M. (2024). UPI frauds: A study on UPI usage, awareness and impact in India. *International Journal of Research in Commerce and Management Studies, 6*(6), 179–197. https://doi.org/10.38193/IJRCMS.2024.6616

Government/official webpages and portals

7. Department of Financial Services. (2024, November 6). *Growth of various modes of digital payment*. Ministry of Finance, Government of India. https://financialservices.gov.in/beta/en/page/growth-various-modes-digital-payment
8. Indian Cyber Crime Coordination Centre. (n.d.). *National Cyber Crime Reporting Portal (NCRP)*. Ministry of Home Affairs, Government of India. Retrieved December 10, 2025, from https://i4c.mha.gov.in/ncrp.aspx
9. Maharashtra Cyber Department. (n.d.). *About Maharashtra Cyber*. Government of Maharashtra. Retrieved December 10, 2025, from https://mhcyber.gov.in/
10. National Payments Corporation of India. (n.d.). *Unified Payments Interface (UPI) product statistics*. Retrieved December 10, 2025, from https://www.npci.org.in/product/upi/product-statistics
11. Open Government Data Platform India. (2022). *Year-wise details of Unified Payments Interface (UPI) frauds from 2020–21 to 2022–23* [Data set]. Government of India. https://www.data.gov.in/resource/year-wise-details-such-unified-payments-interface-upi-frauds-2020-21-2022-23
12. Press Information Bureau. (2024, December 1). *UPI: Revolutionizing digital payments in India*. https://pib.gov.in/PressReleasePage.aspx?PRID=2079544
13. Press Information Bureau. (2025, April 30). *Curbing cyber frauds in Digital India* [Press release]. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=2
14. Press Information Bureau. (2025, March 10). *Digital payment transactions surge with over 18,000 crore transactions in FY 2024–25* [Press release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110405
15. Reserve Bank of India. (2017a, 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) [Notification]. https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336
16. Reserve Bank of India. (2017b, December 14). *Customer protection: Limiting liability of customers of co-operative banks in unauthorised electronic banking transactions* (RBI/2017-18/109; DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18) [Notification]. https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2623

News / magazine / trade press (group author)

17. Economic Times BFSI. (2025, April 3). *How NPCI is looking to combat rising UPI frauds with AI tools*. https://bfsi.economictimes.indiatimes.com/news/fintech/how-npci-is-looking-combat-rising-upi-frauds-with-ai-tools/119961408
18. Fortune India. (2024, November 24). *UPI frauds: 6.3 lakh cases worth ₹485 crore reported in FY25 so far*. https://www.fortuneindia.com/macro/upi-frauds-63-lakh-cases-worth-485-cr-reported-in-fy25-so-far/119275
19. News18. (2025, March 5). *Maharashtra loses Rs 7,634 crore to cyber frauds in one year, Pune reports highest losses*. https://www.news18.com/india/maharashtra-loses-rs-7634-crore-to-cyber-frauds-in-one-year-pune-reports-highest-losses-9251272.html