IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

UPI FRAUD PATTERN ANALYSIS

A Study of Digital Payment Fraud in India's UPI Ecosystem — Causes, Modus Operandi, Regulatory Safeguards, and a Primary Survey of 126 Indian UPI Users with appropriate conclusion.

By: Aarnav Raipancholia,
Student, Senior Year Junior College (XII)
Mithibai College, Mumbai, India

1. Introduction

The Unified Payments Interface (UPI) has become the backbone of everyday money movement in India. Built by the National Payments Corporation of India (NPCI) and regulated by the Reserve Bank of India (RBI), UPI processed a record 24,161.69 crore transactions worth ₹314.23 lakh crore in the financial year 2025-26 alone, serving 55.49 crore onboarded users and accounting for roughly 85% of the country's retail digital payment volume. What began as a convenience feature for splitting bills and paying local shopkeepers has, in under a decade, become critical financial infrastructure.

However, the rapid growth of UPI has also led to an increase in fraud cases. Government data placed UPI-linked fraud at ₹805 crore across more than 10.64 lakh cases in FY26 alone, continuing a multi-year trend that saw UPI fraud losses climb from roughly ₹242 crore in FY22 to ₹1,087 crore in FY24, before easing slightly to ₹981 crore in FY25. A 2025 nationwide survey by LocalCircles found that one in five families with a UPI user had experienced fraud at least once in the preceding three years — and that 51% of those victims never reported the incident at all. This shows that fraud has become a significant challenge alongside the rapid growth and success of digital payments in India.

This project studies that problem specifically as it plays out in India, using only India-specific sources — RBI and NPCI data, Indian news reporting, Indian legal and banking references — and combining that secondary research with an original primary survey of 126 Indian UPI users conducted for this

project. This project aims to understand why UPI fraud happens and how scammers carry it out, explore the protections and prevention methods available to Indian consumers, and use survey responses to understand whether awareness of UPI fraud actually translates into safe behaviour. The project also references an applied tool built alongside this research, UPI Fraud Sentinel, described briefly in Section 10.

2. What Is UPI Fraud?

UPI itself is a real-time payment system, launched by NPCI on 11 April 2016 under RBI's regulatory oversight, that allows instant transfer of funds between two bank accounts using a mobile device. Instead of sharing account numbers or IFSC codes, users transact through a Virtual Payment Address (a UPI ID, such as name@bank) or a QR code, and a single UPI app can be linked to multiple bank accounts. Every transaction that debits money from a UPI-linked account requires the account holder to authorise it, always by entering a UPI PIN.

UPI fraud can be defined as any deceptive scheme in which a person is manipulated into authorising, or unknowingly triggers, a UPI transaction that moves money out of their account without genuine, informed consent or one in which a fraudster obtains a victim's UPI credentials (PIN, OTP, or device/app access) in order to authorise transactions on their behalf.

An important point to understand about UPI is that transactions require authorisation before money can leave a user's account. This means that, unlike a conventional data breach or hacking incident, the overwhelming majority of UPI fraud does not depend on defeating any encryption or banking security system at all. It depends on tricking the account holder into personally supplying that authorisation. This shows that UPI fraud is mainly a social-engineering problem, where scammers trick people into making payments, rather than a failure of UPI's security system itself.

It is also worth separating UPI fraud from the broader category of "bank fraud" that the RBI reports on annually. RBI's annual report data shows overall bank fraud amounts of ₹36,014 crore in FY25 and ₹48,021 crore in FY26, but these totals are overwhelmingly driven by loan and advances-related fraud at the level of individual large accounts, not by UPI transactions. In contrast, UPI fraud involves a much larger number of cases but smaller amounts of money in each case, showing that these scams mainly affect ordinary individual users rather than large corporate accounts.

3. Why Is UPI Fraud Rising in India?

Several structural and behavioural factors, specific to how UPI has grown and how it works, explain why fraud has risen alongside adoption rather than falling as the system matures.

- **Explosive, rapid adoption outpacing financial literacy.** With 55.49 crore onboarded users and UPI now handling around 85% of India's retail digital payment volume, a large share of users are recent, first-time adopters of digital finance, including in smaller towns and among older users who may not intuitively grasp the difference between a "push" (sending money) and a "pull" (a collect request) transaction.
- **Instant, largely irreversible transactions.** Unlike a cheque or an NEFT transfer, UPI payments settle in seconds and funds are frequently withdrawn from the receiving account almost immediately. This removes the natural cooling-off period that slower payment rails provide, and

shrinks the recovery window to what investigators call the "golden hour", the brief period in which a fast complaint can still get a receiving account frozen before the money is moved further.

- **Human psychology, not technology, is the real attack surface.** Cybercrime specialists in India consistently report that fraud rings exploit urgency, fear of an account being blocked or of arrest, impersonated authority posing as a bank, the police, or a government agency, and greed (fake cashback, refunds, or prizes) rather than attacking UPI's underlying security.
- **Cheap, accessible tools for scammers.** Legitimate remote-access software such as AnyDesk or TeamViewer is routinely repurposed by fraudsters; personal data leaked from unrelated breaches feeds targeted social engineering; and there are early signs of AI-based voice cloning and deepfakes being used to impersonate known contacts or officials.
- **Organised laundering through mule accounts.** Once a fraudulent transaction succeeds, stolen funds are typically layered rapidly through a chain of "mule" bank accounts, often opened using stolen or rented identities making recovery difficult once the golden hour has passed.
- **Under-reporting weakens the system's feedback loop.** The 2025 LocalCircles survey found that 51% of UPI fraud victims never reported the incident at all, which not only reduces individual chances of recovery but also limits how much banks, NPCI, and police can learn about evolving fraud patterns.
- **Jurisdictional distance.** A significant share of scam call centres operates from outside the immediate jurisdiction of the local police handling a complaint, which complicates investigation, arrest, and prosecution even when a case is reported promptly.

4. Types of UPI Fraud

The specific tactics fraudsters use in India evolve constantly, but most reported cases fall into a fairly small set of recurring patterns, summarised below.

- **Collect Request ("Pull Transaction") Scam.** A fraudster sends a payment request disguised as an incoming payment. For example, claiming the victim must "approve" a request to receive a refund or prize. Entering the UPI PIN on a collect request always approves an outgoing debit, never a credit. This pattern was so heavily abused that NPCI directed all banks and UPI apps to stop processing person-to-person collect requests UPI-wide from 1 October 2025 although merchant-side collect requests continue to operate under separate limits.
- **Fake or Malicious QR Code Scam.** Scanning a QR code can only ever initiate a payment, it can never be used to receive one. Fraudsters posing as buyers on online marketplaces, or physically pasting fraudulent QR stickers over a legitimate shopkeeper's code, redirect payments to themselves instead of the intended recipient.
- **Fake Customer Care Scam.** Fraudulent "customer care" numbers are seeded on search engines and social media, impersonating banks, wallets, or e-commerce platforms. Callers ask victims to share an OTP or PIN, or to enable screen-sharing, under the pretext of resolving a fake complaint.
- **Screen-Sharing / Remote Access App Fraud.** Victims are persuaded to install applications such as AnyDesk, TeamViewer, or Quick Support, believing they are getting technical help. These apps give the fraudster a live view of or full control over the victim's device during an active banking session.

- **Phishing and Smishing (SMS Phishing).** Fraudulent links imitating a bank's KYC-update page, a refund portal, or a courier-tracking page are sent by SMS or messaging apps, harvesting UPI credentials directly or pushing a malicious app download.
- **SIM Swap Fraud.** Using personal details obtained from data leaks or social media, a fraudster convinces a telecom operator to issue a duplicate SIM in the victim's name, allowing them to intercept OTPs and reset UPI credentials. India's Department of Telecommunications has since introduced a mandatory cooling-off period on SIM replacements specifically to curb this route.
- **Fake or Lookalike UPI Apps and Handles.** Cloned banking apps or UPI IDs that closely resemble a trusted brand's real handle are used to intercept credentials or misdirect payments.
- **"Wrong Number" / Refund and Prize Scams.** A fraudster claims to have transferred money by mistake, or announces a prize or cashback, and asks the victim to "return" or "claim" the amount again via a collect request or PIN entry that actually sends money out.
- **Digital Arrest and Impersonation Scams (related, fast-growing).** Victims receive a call from someone posing as police, the CBI, customs, or another authority, falsely claiming they are under investigation, and are pressured, sometimes over hours or days of continuous video calling into transferring their savings, often via UPI, to "clear their name." This is not strictly a UPI-specific fraud type, but the final payment step is frequently executed over UPI; the Supreme Court estimated nationwide digital-arrest losses at close to ₹3,000 crore for 2025 alone.

5. How Do Hackers Execute UPI Fraud? — The Anatomy of an Attack

Although the scam types in Section 4 look different on the surface, Indian cybercrime investigators consistently describe them as following the same underlying sequence. Understanding these common steps can be more useful than simply memorising different types of scams, as fraudsters may change their methods while following a similar overall pattern.

- **Step 1 — Targeting and data gathering.** Phone numbers and identities are sourced from data leaks, social media profiles, online marketplace listings, or simple random dialling. Organised fraud call centres typically work from scripted lead lists and call scripts.
- **Step 2 — Establishing a pretext and trust.** The fraudster impersonates a bank employee, a delivery agent, a buyer, a government official, or a payment app's customer care representative, often using a spoofed caller ID or a lookalike social media handle to appear credible.
- **Step 3 — Creating urgency or fear.** A threat or a time-limited incentive is introduced specifically to short-circuit the victim's normal instinct to pause and verify.
- **Step 4 — The ask.** Despite the variety of scam types, the actual technical request always reduces to one of a handful of levers: approve a collect request, scan a QR code, read out an OTP or PIN, or install a screen-sharing app.
- **Step 5 — Authorisation and fund movement.** Because UPI transactions require authorisation, the payment is usually completed through the victim's own action, such as entering a PIN or approving a request. In most cases, there is no separate hacking step, and the payment system works as it was designed to.
- **Step 6 — Rapid layering.** Once received, stolen funds are typically moved within minutes through a chain of mule bank accounts to frustrate any freeze request, before the victim has even realised money is missing.

- **Step 7 — Exit and repeat.** The fraudster discards the SIM card or device used for the attack and moves on to the next target, often reusing the same script with only minor variations.

This pattern shows that in most UPI fraud cases, the technology itself is not the main weakness. Instead, scammers usually take advantage of people by creating a sense of urgency and pressuring them into making a decision without thinking carefully. This is precisely the pattern this project's own survey was designed to test directly, with results discussed in Section 9.

6. A Guide to UPI Fraud Prevention

6.1 Habits Before You Pay

One of the most important rules for avoiding many common UPI scams is that a UPI PIN is required to send money, not to receive it. Before entering a PIN, always read the name displayed on the confirmation screen and confirm it matches who you intend to pay, treat any message that says "enter your PIN to receive money" as an automatic red flag, regardless of how official it looks.

6.2 App and Device Hygiene

Install UPI apps only from the Google Play Store or Apple App Store, keep the phone's operating system and banking apps updated, and use a screen lock and app-lock on any device linked to a UPI account. Screen-sharing or remote-access apps such as AnyDesk or TeamViewer should never be installed at the request of an unknown caller, no matter how technical or official the reason sounds.

6.3 Verification Habits

Never trust a customer care number found under a social media complaint or through a general web search, fraudsters routinely seed fake numbers in exactly these places. Instead, use only the number or in-app chat listed on the bank's official website, mobile app, or the back of a physical card or passbook.

6.4 Limits and Alerts

Keep SMS and email transaction alerts switched on for every linked account, and consider setting a lower daily UPI transaction limit through the app's settings if large transfers are not part of routine use. This caps the maximum possible loss from any single successful scam.

6.5 Know the Institutional Safeguards

NPCI's Comprehensive UPI Information Security Framework (CUISF) 2025 and its Mobile Application Security Framework require payment service providers to implement stronger authentication and app-level security controls across the UPI ecosystem, and the discontinuation of person-to-person collect requests from 1 October 2025 has closed one of the most heavily abused loopholes described in Section 4. These are backend protections, but knowing they exist helps in recognising when a request shouldn't be possible in the first place. For example, a genuine P2P collect request can no longer arrive at all.

6.6 Be Ready to Report Before You Need To

Save the national cybercrime helpline number 1930 and the portal cybercrime.gov.in before an incident happens, not after. Because UPI transfers are near instant, the chance of a fraudulent transaction being frozen before the money is withdrawn depends heavily on how fast it is reported. Investigators refer to this narrow window as the **golden hour**.

7. Basic Do's and Don'ts to Avoid UPI Fraud Cases

As a quick reference, the table below distils the prevention guidance from Section 6 and the fraud patterns from Section 4 into a simple two-column checklist.

DO	DON'T
Verify the recipient's name shown on screen before entering your UPI PIN.	Don't share your UPI PIN, OTP, or CVV with anyone, including someone claiming to be "bank staff."
Remember: your UPI PIN is only ever needed to send money, never to receive it.	Don't scan a QR code or approve a collect request in order to "receive" money.
Download UPI apps only from the Google Play Store or Apple App Store.	Don't install AnyDesk, TeamViewer, or similar screen-sharing apps on a stranger's instruction.
Keep SMS and email transaction alerts switched on for every linked account.	Don't click payment, refund, or KYC-update links sent over SMS or WhatsApp by unknown numbers.
Call your bank only on the number printed on your passbook, card, or official website.	Don't search for "customer care" numbers on social media or general web search engines.
Report any unauthorised transaction to your bank and 1930 within minutes, not days.	Don't act on threats of account freezing or arrest without independently verifying with your bank or local police.
Set a comfortable daily UPI transaction limit through your payment app.	Don't stay on a call that insists you keep it secret from your family or your bank.
Keep your UPI app and phone operating system updated at all times.	Don't reuse the same UPI PIN across multiple apps or bank accounts.

Table 1: Quick-reference Do's and Don'ts for UPI users.

8. RBI Guidelines on Unauthorised Transactions

The primary regulatory protection available to Indian bank customers is RBI Circular titled "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," issued on 6 July 2017 and applicable to all scheduled commercial banks, small finance banks, payments banks, and prepaid payment instrument issuers. The circular defines three tiers of customer liability for unauthorised electronic transactions, summarised in Table 2 below.

Liability Tier	When It Applies	Customer's Maximum Liability
Zero Liability	Loss due to bank negligence or a system breach; or a third-party breach reported by the customer within 3 working days of the bank's alert.	None — full amount credited back.

Liability Tier	When It Applies	Customer's Maximum Liability
Limited Liability	Third-party breach reported 4–7 working days after the bank's alert (delay not attributable to the bank).	Capped at ₹5,000–₹25,000 depending on the account or instrument type.
Full Liability	Loss is due to the customer's own negligence (e.g. voluntarily sharing PIN/OTP) and reporting is delayed beyond 7 working days.	Entire loss borne by the customer.

Table 2: RBI's three-tier liability framework for unauthorised electronic banking transactions.

Two procedural safeguards accompany these liability tiers. First, once a customer notifies the bank of an unauthorised transaction, the bank must provisionally credit the disputed amount back to the customer's account within 10 working days of that notification, without waiting for the outcome of any insurance claim. Second, the bank is required to resolve the complaint within a maximum of 90 days.

There is one important point to consider specifically for UPI transactions. Most of the fraud types described in Section 4 involve the victim personally entering their own UPI PIN after being deceived. Technically, an authorised transaction in the strict sense used by the circular, even though the victim did not intend or understand what they were authorising. Banks and courts have generally treated this pattern as customer side negligence rather than a pure unauthorised transaction, which limits how much protection the zero liability rule provides once PIN based authorisation has actually occurred. This is why preventing UPI fraud is often more important than relying on recovery after the money has already been transferred.

Beyond the 2017 circular, RBI and NPCI continue to add safeguards specific to UPI. Risk-based transaction limits, protections against unauthorised mobile-number changes and SIM-based authentication misuse, and tightened security requirements for UPI applications, as reiterated by the Ministry of Finance in 2026.

9. Primary Research: Survey of 126 UPI Users in India

9.1 Methodology

A self-administered, 14 question Google Forms questionnaire was circulated among UPI users between 3 and 7 August 2026, gathering 126 valid responses. The questionnaire covered usage patterns, prior exposure to suspicious activity, awareness of common UPI fraud types, self-assessed knowledge of fraud prevention, and, critically, a scenario-based question that tested actual decision making against a simulated enter your PIN to receive money scam, the exact mechanic behind the collect request and QR-code scams described in Section 4. All individual responses have been aggregated for this analysis. No personally identifying information from the raw responses is reproduced here.

9.2 Respondent Profile

The sample skews toward established, frequent UPI users rather than first-time or teenage users: half of respondents were aged 45–55, and 77% use UPI multiple times a day. This is a useful population to study

precisely because these respondents are often assumed by themselves and others to be experienced and cautious digital payment users, which makes the gaps identified below more, not less, notable.

Age Group	Share of Respondents	UPI Usage Frequency
45–55 years	50% (n = 63)	Multiple times a day — 77%
35–44 years	25.4% (n = 32)	A few times a week — 9.5%
25–34 years	23% (n = 29)	Once a day — 5.6%
56 years and above	1.6% (n = 2)	Never / Rarely — 8%

Table 3: Age and usage-frequency profile of survey respondents (n = 126).

9.3 Awareness of UPI Fraud and Exposure to Suspicious Activity

96.8% of respondents said they were already aware, before taking the survey, that UPI fraud is becoming increasingly common in India, closely matching the near total awareness one would expect given how heavily this topic is covered in Indian media. But awareness of the trend in the abstract has clearly not been enough to prevent direct exposure. 53.2% of respondents had personally received a suspicious UPI related call, message, QR code, or payment request, and 12.7% had actually been victimised by a UPI-related fraud or financial scam at some point.

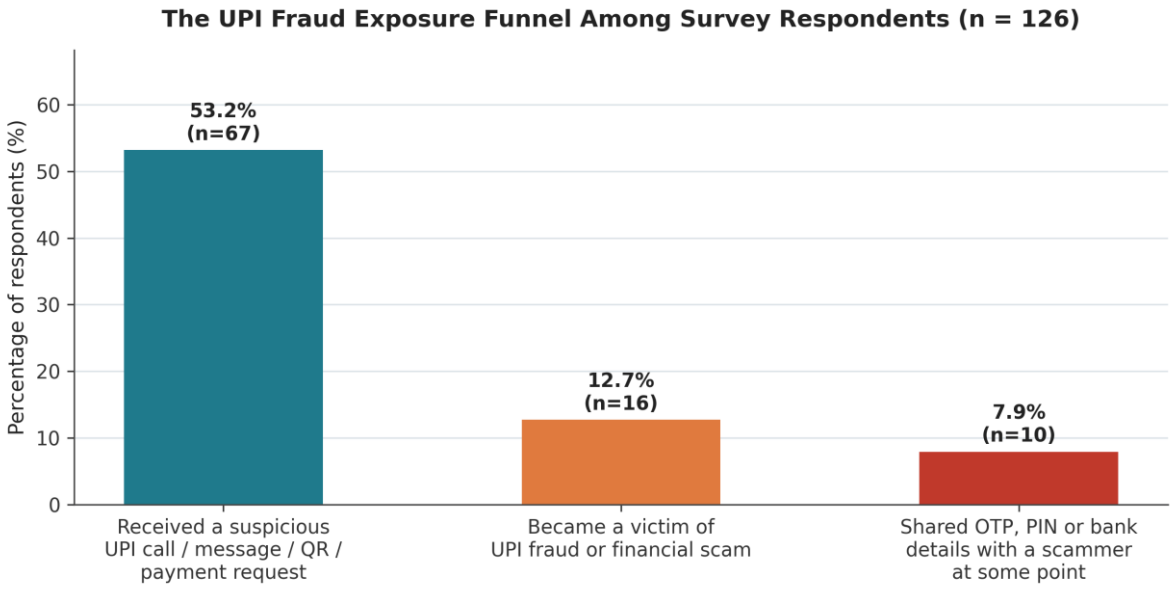


Figure 1: The exposure funnel from suspicious contact to victimisation to credential-sharing among survey respondents.

It is worth noting that victimisation was not confined to respondents who could clearly recall a suspicious contact. Four of the sixteen victims had answered "not sure" when asked whether they had received a suspicious request, suggesting that some fraud attempts are subtle enough that victims do not recognise them as suspicious even in hindsight.

9.4 Where Awareness Comes From

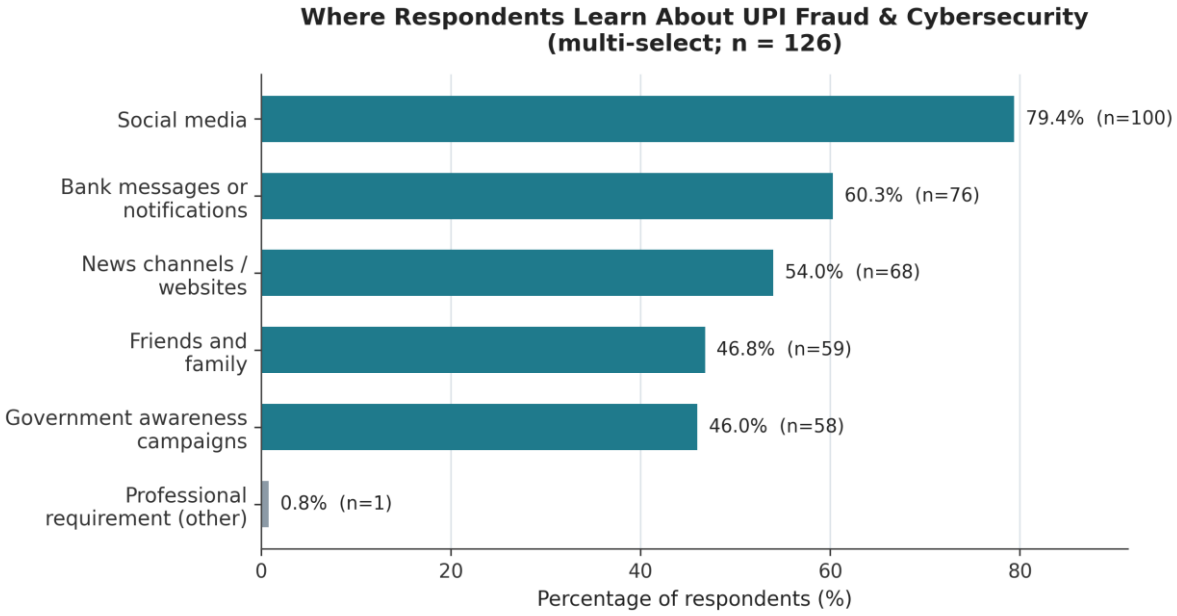
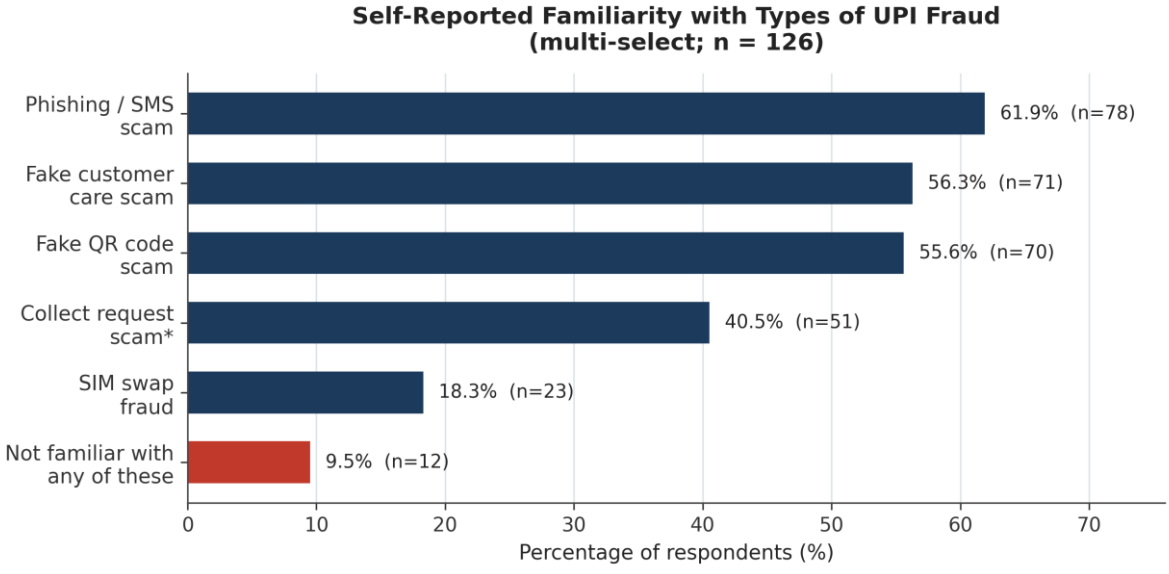


Figure 2: Sources respondents rely on to learn about UPI fraud and cybersecurity (multi-select).

Social media was, by a wide margin, the single largest source of fraud awareness, ahead of direct bank messages or notifications and news media. Government awareness campaigns reached under half of respondents, a similar share to informal word of mouth through friends and family. This suggests there is still room for official campaigns to close the gap with informal channels, which offer wide reach but no guarantee of accuracy.

9.5 What Fraud Types Are Actually Recognised



**Collect request scam remained a familiar term even though NPCI discontinued P2P collect requests on UPI from 1 October 2025 as a fraud-prevention measure.*

Figure 3: Self-reported familiarity with named UPI fraud types (multi-select).

Phishing/SMS scams, fake customer care scams, and fake QR code scams were the most recognised fraud types among respondents. Interestingly, 40.5% still named the "collect request scam" as one they recognised, even though NPCI discontinued person to person collect requests UPI wide from 1 October 2025 specifically because this feature was so widely abused. This most likely reflects lingering awareness built up before the rule change, continued exposure to the equivalent pattern through merchant side collect requests which the ban did not cover, or simply that the underlying trick "enter your PIN to receive

money" still persists in other forms even where the original collect-request mechanism has been switched off. SIM swap fraud was the least recognised named type, and 9.5% of respondents said they were not familiar with any of the listed fraud types at all, a small but meaningful group with essentially no named baseline defence against social engineering attempts.

9.6 The Confidence Gap

This is arguably the most important finding of the survey. 79.4% of respondents rated their own knowledge of UPI fraud prevention as "Good" or "Very Good," and 96.8% correctly answered, in the abstract, that entering a UPI PIN authorises a payment and should never be shared. Yet when presented with a realistic scenario: "If you receive a request claiming you will receive money after entering your UPI PIN, what would you do?", only 85.7% selected the objectively correct response "Reject the request", while 6.3% said they would either enter the PIN or were unsure what to do.

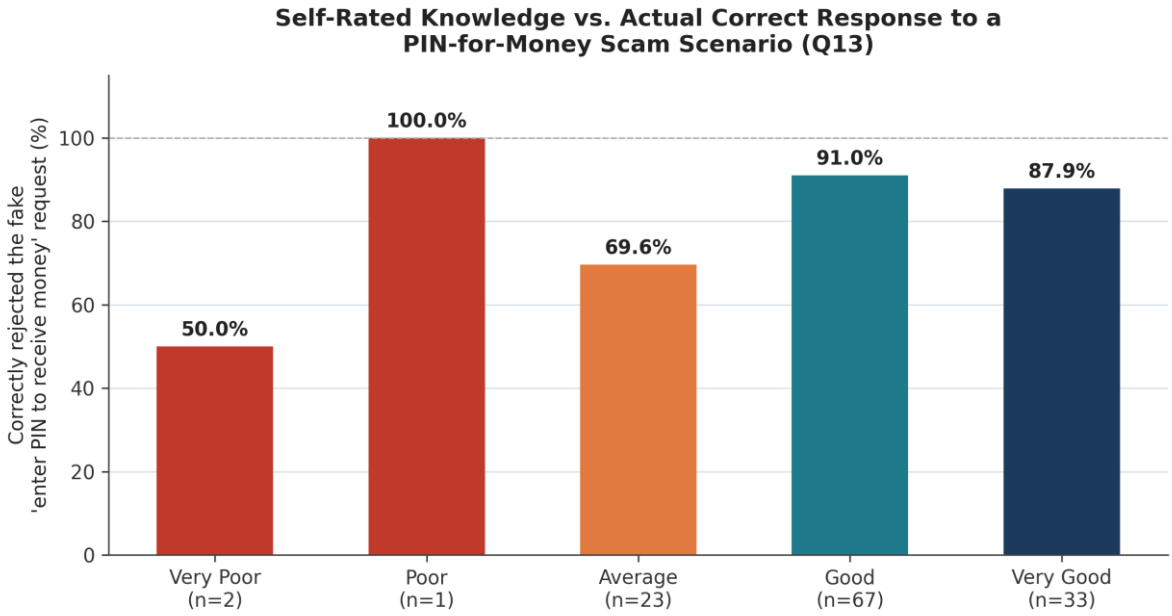


Figure 4: Self-rated knowledge of UPI fraud prevention compared with the actual correct-response rate to a simulated PIN-for-money scam.

Correct responses generally rose with self-rated knowledge, but not cleanly. Among respondents who rated their own knowledge "Very Good," 12.1% still did not choose the safe response and this group's correct response rate was actually lower than that of respondents who rated themselves only "Good", even though the two groups answered the more basic, abstract PIN authorisation question almost identically. This pattern may suggest that some respondents were overconfident about their ability to identify UPI fraud. It also shows that knowing about fraud does not always mean that a person will make the right decision in a real situation. The "Poor" and "Very Poor" self-rating groups contained only one and two respondents respectively, too few to draw firm conclusions from in isolation, and are shown in Figure 4 for completeness rather than as a robust trend.

9.7 Sharing Behaviour and Reporting

7.9% of all respondents admitted to having shared an OTP, bank account detail, or another sensitive credential with someone falsely claiming to be from a bank, payment app, or government body at some point, a group that only partly overlaps with the 16 confirmed victims, suggesting some near misses were caught before money was actually lost. Among the confirmed victims, reporting behaviour was mixed. 68.8% reported the incident to their bank, cybercrime authorities, or both, while 31.2% did not report it

at all. This under reporting rate, while lower than the 51% figure found in the 2025 LocalCircles national survey, still points in the same direction. A meaningful share of UPI fraud in India goes unreported even among people who recognise they were victimised, which limits both individual recovery chances and the system's overall visibility into evolving fraud patterns.

9.8 Key Takeaways from the Survey

- **Awareness does not equal protection.** Most respondents were aware that UPI fraud is common, but many had still received suspicious requests or experienced fraud themselves.
- **Informal channels dominate awareness-building.** Social media reaches more respondents than bank alerts, news media, or government campaigns combined with any single official channel, useful for reach, but not a substitute for accurate, verified information.
- **Newer or less publicised vectors remain under recognised.** SIM swap fraud, despite being capable of causing very large losses, was recognised by fewer than one in five respondents.
- **Confidence is a weak predictor of correct behaviour.** Self-rated "Very Good" knowledge did not translate into the highest correct response rate on a realistic scenario question, a finding with direct implications for how prevention messaging and tools should be designed.
- **Under reporting persists even among victims.** Nearly a third of confirmed victims in this sample did not report the incident at all, echoing the pattern found in larger national surveys. This might spark concern and a call for more awareness campaigns shall be required now as well as in the near future.

10. Applied Component: The UPI Fraud Sentinel Tool

To translate the patterns studied in this project into something practically useful, this research is accompanied by a browser based tool built as part of the same project, UPI Fraud Sentinel. It is a self contained web application, requiring no server or account, that applies a transparent, rule based scoring framework to flag transaction patterns statistically associated with the fraud types discussed in Section 4. For example, unusually round amounts sent to freshly created payee handles, rapid repeated payment attempts, or a mismatch between an entered name and the actual registered account name. The tool includes a live transaction calculator for testing individual payments, a bulk upload option for checking many transactions at once, and a plain language awareness section that mirrors the Do's and Don'ts checklist in Section 7 for a general audience.

The tool is deliberately kept rule based (9 rules provided by the NPCI) and transparent rather than built as an opaque machine learning model. Every flagged transaction can be traced back to the specific rule that triggered it, which makes the logic inspectable, teachable, and easy to refine as new scam patterns emerge. This approach also fits the main idea of this project: many fraud attempts follow recognisable behavioural patterns.

The website can be accessed with the following link: upifraudsentinel.netlify.app

11. Conclusion

UPI has transformed how India moves money, reaching a scale 24,161.69 crore transactions worth ₹314.23 lakh crore in FY26 alone with no real precedent anywhere else in the world. However, some of the features that make UPI convenient, such as instant transfers and quick payments through mobile apps, can also be misused by fraudsters to target users. As discussed in Sections 4 and 5, the technology itself is usually not the main weakness. In many cases, fraud occurs when scammers pressure or manipulate people into making decisions quickly without properly verifying the request.

India's regulatory response has measurably closed specific loopholes: RBI's 2017 zero-liability framework gives customers a genuine, time bound path to recovery in cases of bank or third-party negligence, and NPCI's discontinuation of P2P collect requests from October 2025, alongside its Comprehensive UPI Information Security Framework, has removed one of the most heavily abused attack vectors described in this paper. Yet new methodologies such as the discussed SIM swap fraud, remote access app scams, and increasingly, AI assisted impersonation and "digital arrest" schemes continue to emerge and adapt around each fix.

The survey conducted for this project also supports many of the findings from the secondary research. Although most respondents were aware of UPI fraud, this awareness did not always lead to the correct response when they were presented with a realistic scam situation. The gap between knowing about fraud and responding safely in an actual situation is an important challenge. Awareness campaigns, security measures, and tools such as UPI Fraud Sentinel should focus on helping people apply this knowledge in real situations.

One of the most important lessons from this project is that a UPI PIN is only required to send money and never to receive it. No genuine bank, government official, or customer care representative will ask for a UPI PIN over a call, message, or screen-sharing session.

12. References

All sources consulted for this project are India-specific — Reserve Bank of India and NPCI publications, Indian government press releases, and Indian news, legal, and banking sources.

1. Business Standard. "Legacy cases lifted bank fraud to ₹48,021 cr in FY26: RBI annual report." 29 May 2026.

2. Business Standard. "Bank fraud cases fell in FY25, amount rose threefold to ₹36,014 cr: RBI." 30 May 2025.

3. Business Standard. "Bank frauds rise 166% in FY24 to over 36,000 cases, shows RBI annual report." 30 May 2024.

4. Madhyamam. "UPI-linked frauds amount to Rs 805 crore so far in FY26: Govt." 15 December 2025.

5. The420.in. "₹805 Crore Lost to UPI Frauds This Year, Government Says." December 2025.

6. Business Standard. "1 in 5 UPI users faced fraud; 51% victims didn't report, reveals survey." 26 June 2025.

7. Press Information Bureau, Government of India. "UPI completes 10 glorious years, Emerges as World's Largest Real-Time Payments Platform." 30 April 2026.

8. ANI / New Kerala. "UPI user base reaches 55.49 crore; FY26 transactions rise to 24,162 crore worth Rs 314 lakh crore." 20 July 2026 (citing Ministry of Finance / NPCI data).

9. Business Today. "NPCI to tighten UPI rules: Peer to peer collect feature to end in October." 13 August 2025.

10. Ujjivan Small Finance Bank. "Common UPI Scams in India and How to Avoid & Stay Safe."

11. The420.in. "UPI Fraud: How Cybercriminals Are Exploiting India's Digital Payments System." 12 March 2026.

12. Razorpay. "UPI Fraud: Common Types and Methods to Prevent UPI Payment Scams."

13. Nest App. "UPI Safety Tips India: How to Avoid UPI Fraud and Scams." 18 April 2026.

14. IDFC FIRST Bank. "6 Types of UPI Frauds & How to Stay Safe."

15. The420.in. "Phishing, UPI Scams and Remote Access Fraud on the Rise, Experts Warn."

16. Reserve Bank of India. Circular RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18, "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions." 6 July 2017. rbi.org.in.

17. Share India. "RBI Guidelines on Unauthorised Transactions: Customer Liability, Refund Rules & Safety Measures."

18. Sachar Law Firm. "Unauthorised Bank Transactions: When Customers Have Zero Liability Under RBI Rules."

19. Advocate Mridul Jindal. "Zero Liability on Card Fraud — RBI's 3-Day Rule Explained." 30 June 2026.

20. Simple English Wikipedia. "1930 (Indian Cybercrime Helpline)."

21. ApniLaw. "Cyber Crime Helpline 1930 – How It Works in India." 17 March 2026.

22. Shankar IAS Parliament. "CERT-In: India's Frontline Defender against Cyber Threats." January 2026.

23. ScamWatchHQ. "India Scams 2026: Fake Cops, Deepfake Tycoons, and the ₹22,500-Crore Fraud Epidemic Riding the World's Biggest Payments Rail." 6 June 2026.

24. The Quint (My Report). "'Scammed of Rs 25 Lakh, I'm Now Dependent on My Children in Old Age': Senior Citizen Shares Ordeal."