International Journal of Multidisciplinary Research and Development
www.allsubjectjournal.com
ISSN Online: 2349-4182 ISSN Print: 2349-5979
Received: 26-09-2025, Accepted: 26-10-2025, Published: 10-11-2025
Volume 12, Issue 11, 2025, Page No. 53-58

Phishing in India's Fintech Era: Liability, enforcement, and consumer trust

Jasmine Sharma
Bar Council of Delhi, Delhi District Courts, Delhi, India

Abstract
Phishing in the FinTech era has transformed from isolated cyber tricks into a systemic threat that challenges law, regulation, and consumer protection. India's digital payments ecosystem—led by UPI and handling nearly half of the world's real-time transactions—has expanded at record speed, but its legal architecture has not kept pace. The result is a troubling paradox: while technology delivers speed and scale, it also enables "authorised but fraudulent" transfers that blur traditional categories of negligence, deception, and service deficiency. Victims are left navigating fragmented remedies across criminal law, consumer forums, and RBI circulars, often with inconsistent outcomes.

This paper examines that gap. It traces the anatomy of phishing in FinTech, reviews India's patchwork legal framework, and analyses how courts, regulators, and consumer commissions currently allocate liability. Comparative study of the EU's PSD2, the UK's reimbursement model, and U.S. Regulation E highlights alternative policy choices, from prevention by design to socialised risk-sharing. A key insight is that India's system lacks both clarity of liability rules and the institutional capacity to investigate frauds quickly. Forensic bottlenecks—such as weak blockchain tracing, delays in mutual legal assistance, and evidentiary hurdles under Section 65B of the Evidence Act—mean that even strong liability laws will struggle without enforcement support.

The article argues for statutory recognition of authorised-but-fraudulent transfers, default reimbursement rules, stronger authentication standards, and a unified FinTech fraud response authority. By linking comparative lessons with India's forensic realities, it charts a reform path to safeguard consumers, stabilise trust, and preserve innovation in the digital economy.

"Trust is the currency of the digital economy. Once it is broken, no technology can replace it." - Christine Lagarde, President, European Central Bank.

Keywords: Consumer protection, cybercrime, digital payments, fintech regulation, phishing, regulatory gaps

Introduction

The FinTech revolution has changed how millions pay, borrow, and save. In India, digital payments have exploded. By early 2025, more than 18,000 crore transactions had already been recorded in FY 2024–25, covering everything from small kirana store purchases to big online sales. The Unified Payments Interface (UPI), the backbone of this system, was set a target of about 20,000 crore transactions for the year. This shows how serious policymakers are about making instant, low-cost payments available nationwide. What's striking is that this growth isn't just local—it's global. The Reserve Bank of India noted that UPI alone handled nearly 48.5% of all real-time payment transactions worldwide in FY 2024–25, making it the largest such system anywhere. But speed also brings risks. According to the RBI's Annual Report 2024–25, while the number of certain fraud cases declined, the total money lost to fraud rose sharply. Reports highlight that internet and card fraud cases dropped, yet big-ticket frauds and re-classifications pushed overall banking losses much higher.

This global picture is mirrored outside India. The FBI-run Internet Crime Complaint Center (IC3) recorded 859,532 complaints in 2024, with total reported losses of about USD 16.6 billion, and identified phishing/spoofing among the top complaint categories. Older adults were disproportionately harmed: IC3 reported that people aged 60+ lodged large numbers of complaints and accounted for billions in losses. These American figures echo a worldwide pattern: phishing and social-engineering scams remain the highest-volume threat to online financial trust.

Why does this matter for law? Because phishing in the FinTech era often produces authorised-looking transfers - victims are tricked into entering credentials or approving transactions -which complicates traditional legal categories. Criminal statutes such as the Information Technology Act, 2000 [10, 14] (identity theft and personation provisions) provide tools to punish perpetrators; administrative instruments like the RBI's customer-protection circulars set operational rules for banks and payment service providers; and consumer law (the Consumer Protection Act, 2019) offers a remedial forum for customers alleging deficiency of service.

Different countries have taken different paths in tackling payment fraud. In the EU, the PSD2 rules focus on prevention by setting strict customer authentication standards and making providers clearly responsible. The UK, on the other hand, has started requiring banks to reimburse victims of certain "authorised push payment" scams. In the U.S., the approach is more mixed laws like the Electronic Fund Transfer Act and Regulation E, along with enforcement agencies, combine consumer protection with duties on customers to report fraud. The central legal problem is therefore urgent and concrete: when a FinTech-enabled payment is induced by a phishing scam, who bears the loss -the consumer, the bank/FinTech, or some shared socialised model -and on what legal basis? Without clear, predictable allocation rules, victims face slow redress, providers face uncertain duties, and public trust -the currency of FinTech erodes.

While policy reports and regulatory documents abound, systematic legal scholarship on phishing in India's Fin Tech

sector remains sparse. Existing studies tend to focus either on the technological mechanics of fraud or on broad consumer protection issues without engaging with the unique challenges of "authorised but fraudulent" transactions. Academic commentary from Europe and the United Kingdom has debated allocation of liability in authorised push payment scams, but Indian scholarship has not yet fully addressed how doctrines under the Information Technology Act, Consumer Protection Act, and RBI circulars interact in real phishing disputes. This article therefore seeks to fill a gap in the literature by situating phishing within India's evolving FinTech law and by drawing on comparative models to highlight possible reform pathways.

This article proceeds to analyze that question. It synthesizes statutory law, RBI and regulatory guidance, consumer-forum decisions, and comparative frameworks to show where gaps persist and how the law can be re-designed to prevent harm, compensate victims swiftly, and preserve an experimentation-friendly environment for FinTech innovation.

1. Anatomy of Phishing in the FinTech Ecosystem

Phishing in the FinTech era is no longer a lone email scam-it is an evolving modus operandi that exploits the architecture of modern payments systems: instant rails (UPI, IMPS), tokenised wallets, third-party apps, and crypto on-ramps. Attackers now mix social engineering, technical exploits (e.g., SIM swap, malicious QR codes), and business-model deception (fake lending apps, impersonation of payment aggregators) to convert trust into an instruction to transfer funds.

These murky mechanics create a triage problem for law and regulation:

1. **Mass scale & speed:** massive volumes move within seconds.
2. **Seemingly "authorised" transfers:** the victim is tricked into entering credentials or consenting to a transaction, so the ledger shows the flow as valid.
3. **Rapid layering of funds:** once captured, funds are routed through wallets, mule accounts, or crypto mixers before authorities can intervene.

NPCI itself has repeatedly issued UPI circulars and guidelines acknowledging risks around QR, tokenization, and collect requests, reflecting how central these vectors have become in the Indian payment's ecosystem.

Over time, three phishing patterns have become dominant in FinTech

- Collect-request / QR lures: Fraudsters send a collect request or QR code via WhatsApp/SMS. When the user authorises the request or scans the QR, the payer's account is tapped. NPCI's operations, via UPI circulars and enforcement briefs, acknowledge the prevalence of such tactics.
- Credential / OTP capture attacks: Through SIM swap, phishing links, or fake KYC portals, attackers capture a one-time password or login credential and then complete transfers that appear to be user-authorized.
- Crypto wallet/seed-phrase scams: Victims are fooled into giving away their private keys or approving fake wallet transactions, which lets fraudsters instantly empty their accounts. In some U.S. cases, agencies have shown how such phishing quickly turns into cross-border money laundering through decentralized exchanges.

These scams are legally tricky because the payments often look like they were "authorised" by the victim. That makes it hard to apply traditional criminal or civil rules. Questions about intent, impersonation, or negligence get complicated. It's not always clear if the victim was coerced or deceived, or if the bank or payment service provider failed to keep things secure. These mixed features show why old rules—like strict bank liability for unauthorized transfers or "buyer beware"—don't fit well with modern FinTech phishing.

Table 1: Phishing Attack Vectors in FinTech

Attack Type	Method	Example	Legal Challenge
QR/Collect Request Fraud	Fraudster sends fake request or QR	User authorises unknowingly	Appears as "valid" user-approved transfer
Credential/OTP Capture	SIM swap, fake KYC portals, phishing links	OTP entered on fake site	Courts struggle with "negligence" vs. deception
Crypto Wallet/Seed Phrase Theft	User tricked into giving private keys	Wallet emptied instantly	Cross-border laundering, hard to trace

2. The Existing Legal Architecture: Statutes, Rules, and Soft Law

a. India's Domestic Law – A patchwork

India currently confronts FinTech phishing via multiple legal strands-none designed for this hybrid domain.

- Under the Information Technology Act, 2000, sections 66C (identity theft) and 66D (cheating by personation) form the backbone of cyber fraud enforcement.
- The Consumer Protection Act, 2019 [11,15] treats "financial services" as services liable for deficiency and unfair trade practices, enabling consumer redress for service failures.
- On the sectoral side, the RBI's supervisory circulars (e.g., limiting customer liability in unauthorized electronic transactions) and the PPI / Payment Aggregator guidelines set operational guardrails for banks and digital intermediaries.

Yet these strands remain fragmented. Criminal law addresses the bad actor but offers no fast relief to victims. Consumer law offers compensation but is slow. RBI's circulars (administrative vehicles) depend on factual compliance: timely reporting, internal bank controls, proof of customer "contribution" to loss.

b. Comparative Anchors: PSD2 and UK reimbursement models

Europe's PSD2 introduced prescriptive requirements: Strong Customer Authentication (SCA) for customer-

initiated payments and clear liability allocation rules, shifting responsibility toward payment service providers unless customer fault is established. In the UK, the Contingent Reimbursement Model (CRM) code and newer PSR moves toward mandatory reimbursement in authorized push payment (APP) frauds adopt a loss-sharing strategy: prevention plus compensation. These two models contrast "prevention by design" and "socialisation of residual risk." For India, they serve as contrasting policy archetypes: either force safer design or share loss among the ecosystem when design fails.

To clarify how India's patchwork compares internationally, the following table synthesizes liability allocation models across major jurisdictions, highlighting the different ways regulators have approached phishing-induced transfers.

Table 2: Comparative Liability Models in FinTech Phishing

Jurisdiction	Core Legal Instrument	Approach to Liability	Consumer Protection Outcome	Key Takeaway for India
India	Information Technology Act, 2000; Consumer Protection Act, 2019; RBI Customer Liability Circulars	Fragmented—banks liable only if customers report promptly and did not share credentials	Inconsistent—forums vary between protecting consumers and penalizing user "negligence"	Needs statutory clarity and harmonization
European Union (EU)	PSD2 (Directive (EU) 2015/2366) [6, 17]	Strong Customer Authentication (SCA); liability shifts to providers unless gross negligence	Consumers generally reimbursed if authentication rules followed	Prevention by design + clear allocation
United Kingdom (UK)	CRM Code; Payment Systems Regulator reforms (2023–25)	Mandatory reimbursement for most "Authorised Push Payment" frauds	Shared liability between PSPs and banks; strong consumer confidence	Socialisation of risk + predictable redress
United States (US)	Electronic Fund Transfer Act (EFTA), Regulation E	Liability capped if consumer reports within set timelines	High awareness of reporting duties; regulator-driven enforcement	Mixed model—consumer diligence + regulatory oversight

3. Liability: How Courts, Regulators, and Industry Allocate Loss

The central legal question: Who pays when phishing succeeds? Liability analysis generally divides into three actors: (1) consumer conduct (negligence or fault); (2) PSP obligations (security and redress); and (3) intermediaries (e.g., telecom, app stores).

In India, RBI's customer-protection circulars establish a quasi–safe harbour: if customers report quickly (within prescribed windows), and if they did not share credentials, liability may be limited. But banks must also show they exercised due diligence to get full immunity. In practice, consumer forums flip outcomes depending on whether deadlines were met, evidence of OTP sharing, or bank response delays. In some orders-for example, the Navsari consumer commission forced SBI to refund UPI fraud losses where the bank delayed blocking. In another Noida case, a bank was fined for failing to act after timely notice.

Indian courts have not yet developed a consistent doctrine on liability for phishing-induced transfers. Consumer commissions frequently oscillate between a strict duty on banks to secure systems and a negligence-based approach that penalizes users for sharing credentials, even under deception. For instance, in *State Bank of India v. Suresh Babulal Vora*, the Gujarat State Consumer Commission held the bank liable for failing to block fraudulent UPI transactions despite prompt notice from the consumer, stressing that systemic safeguards are part of a bank's service obligations. By contrast, in *Punjab National Bank v. Leader Valves Ltd.*, the National Consumer Disputes Redressal Commission emphasized customer negligence where credentials were voluntarily disclosed, even under pretext. These conflicting strands highlight the doctrinal uncertainty: is phishing to be treated as a service deficiency, a criminal deception, or a mixed fault-based tort? Without clearer statutory guidance, judicial outcomes remain fact-sensitive and unpredictable.

However, courts tread carefully when consumers plausibly claim deception: tribunals often hold that user sharing of credentials or OTP after a convincing pretext constitutes contributory negligence. That "fault-sensitive" approach creates case-by-case unpredictability. Such variability is precisely what drives industry codes like the UK CRM: instead of litigation by anecdote, a regulated reimbursement structure with behavioral thresholds.

In sum: the Indian model is currently a litigious dance between asserting strict duties and pleading user fault-a mix that lacks clarity and predictability. Only clear statutory or regulatory defaults (for example, presumption of reimbursement unless gross negligence) can replace this ad hoc allocation.

4. Enforcement & Institutional Challenges

Phishing frauds expose deep institutional friction.

Fragmentation is primary: multiple agencies-CERT-In (cyber incident response), FIU-IND (financial intelligence), RBI (payment supervision), NPCI (rail operator), state cyber cells, consumer commissions-operate parallel mandates without unified coordination. FIU-IND's AML/CFT mandates and CERT-In's incident reporting are formidable on paper, but in phishing cases where funds move rapidly, coordination is too slow.

Forensic and cross-border hurdles are equally daunting. Modern frauds spread across jurisdictions, wallets, and crypto platforms. The DOJ's major crypto forfeiture cases show that U.S. law enforcement can trace complex chains-but only with intensive chain-analysis, subpoenas, MLATs, and cooperation. For Indian agencies tracing out-of-country wallets, delays in MLATs and limited chain data sharing reduce real-time efficacy.

Victim underreporting further handicaps enforcement. Many victims do not file complaints due to complexity, fear, or belief that the loss is irrecoverable. A LocalCircles survey reports that "one in five UPI users faced fraud in the past three years," and about 51% of victims did *not* file complaints. Without comprehensive reporting, patterns remain hidden, regulatory design remains reactive, and public confidence erodes.

Beyond these institutional hurdles, the effectiveness of any liability or reimbursement regime ultimately depends on whether authorities can collect, preserve, and present digital evidence promptly - a dimension where forensic gaps remain significant. Phishing frauds also strain forensic capacity. First, digital evidence collection remains inconsistent: Indian cyber cells often lack the tools for blockchain tracing, metadata capture, or SIM-swap forensics. Evidence is frequently challenged in court on grounds of authenticity or chain of custody, delaying prosecutions. Second, international tracing requires cooperation with crypto exchanges and foreign banks, but mutual legal assistance treaties (MLATs) can take months—by which time funds are laundered through multiple accounts or mixers. Third, admissibility standards under the Indian Evidence Act (especially for electronic records under Section 65B) create hurdles when certificates are missing or delayed. Comparative jurisdictions such as the U.S. have developed chain-analysis techniques and rapid subpoena powers to overcome these hurdles, while the EU's Europol framework facilitates near-real-time intelligence exchange. Unless India strengthens forensic infrastructure and harmonises evidentiary rules, even robust liability laws may fail in practice, as perpetrators will remain beyond the reach of enforcement.

5. Reform Roadmap: Law, Regulation, and Design

To be defensible, any reform must align with three legal-policy goals: (1) protect consumers; (2) maintain innovation incentives; (3) allocate enforcement and liability costs justly.

1. Statutory and Regulatory Fixes

- Authorized-but-fraudulent transfer recognition: codify that a transfer induced by fraud (even if authorised) is legally rescindable and subject to civil/regulatory redress (akin to APP fraud laws).
- Mandated SCA-equivalents for high-risk flows: require PSPs to deploy multi-factor authentication or risk-based challenge for large UPI transfers, wallet exits, merchant onboarding.
- Default reimbursement regimes: introduce a statutory presumption that PSPs reimburse victims unless gross user negligence is established. Provide a streamlined appeal process and strict timelines for interim freezing.

2. Institutional Reforms

Create a Single FinTech Fraud Response Authority (FFRA) - a statutory hub combining RBI, NPCI, FIU-IND, CERT-In, and law enforcement liaisons. FFRA's mandate would include real-time triage of reported frauds, emergency freezing orders, chain analytics facilitation, cross-border cooperation coordination, and a centralized complaint portal.

3. Technological & Market Reforms

- Design controls: mandate display of payee legal name before transfer, real-time anomaly detection, transaction risk scoring, and mandatory alerts for high-value transfers.
- Fraud-intelligence exchange: anonymised, regulated shared databases of fraud indicators across PSPs to block known bad actors.
- KYC/AML tightening: impose stricter on-ramps for custodial wallets and nonbank PPIs, including mandatory pause powers and transaction-level thresholds for review.

4. Consumer Education & Low-Friction Remedies

Make reporting easier with a single "Report Fraud" button in UPI or payment apps, and automatically freeze large suspicious transactions. Require clear warnings when users join, like "never share your OTP or seed phrase." Also, set up a shared compensation fund, paid for by payment providers, to quickly help victims while cases are resolved.

Phishing in FinTech isn't just a cyber problem, it's also about who's responsible and how systems are managed. India's current approach is scattered, with old laws and RBI rules that don't always deter fraud. Other countries show that combining strong security rules with reimbursement policies works better. For India, a mix of strict controls, automatic reimbursement, and a single enforcement agency could build trust and protect both users and innovators.

Conclusion

India's FinTech ecosystem is growing at a breathtaking pace. In 2024-25 alone, the country recorded over 18,120 crore digital payment transactions, handling some of the world's largest volumes of real-time payments. Yet, this rapid growth has begun to test the limits of the country's legal and regulatory framework. While internet and card-related frauds fell sharply during the year, more serious forms of phishing and payment scams surged, causing losses of around ₹36,014 crore in bank frauds, nearly three times higher than the previous year. These numbers are more than alarming; they reveal a structural imbalance. The technology enabling instant payments, micro-transactions, and seamless digital credit has far outpaced the legal system meant to oversee it. When phishing attacks manipulate digital payments, victims are often left to navigate a fragmented patchwork of statutes, RBI circulars, consumer forum decisions, and ad hoc institutional remedies. As this analysis shows, phishing now sits in a gray area of the law, part deception, part authorization, part technical failure, making traditional legal rules poorly equipped to respond. A central question remains: who is responsible when a phishing attack succeeds? Courts and regulators in India fluctuate between blaming users for negligence and holding banks or payment providers strictly accountable. Some consumer commissions have ordered banks to refund UPI fraud victims, while others deny compensation when users appear complicit. This inconsistency undermines trust and weakens deterrence. By contrast, international models like the EU's PSD2 with its Strong Customer Authentication rules, or the UK's emerging reimbursement rules for authorized push payments, show that clear legal design can manage risk while building consumer confidence.

The enforcement challenge is equally daunting. Rapid digital transactions, cross-border transfers, and anonymity via crypto wallets make tracing stolen funds urgent but difficult. India's agencies, RBI, NPCI, CERT-In, FIU-IND, and cyber police units largely operate in silos, with no single authority to coordinate complaints, freezes, or forensic investigations. Even when victims report fraud, delays often mean the trail has gone cold. Mutual legal assistance and chain-analysis tools are underused, allowing illicit proceeds to disappear. To address these gaps, reforms need to be bold

and forward-looking. Lawmakers should recognize "authorized-but-fraudulent" transfers as actionable, mandate strong authentication for high-risk transactions, and set clear reimbursement rules for victims where there is no gross negligence. A unified National FinTech Fraud Response Unit could bring together regulators, enforcement agencies, and forensic teams to respond quickly. Technical safeguards like real-time alerts, payer-name disclosures, anomaly detection, and stricter AML/KYC rules should be standard, alongside consumer-friendly features such as a single "report fraud" button, plain-language onboarding warnings, and guaranteed response timelines. Such measures do more than shift liability; they reshape incentives. FinTech companies will prioritize security, banks will act faster, and consumers will have a clear path to redress. As this article has shown, comparative models in the EU, UK, and U.S. demonstrate clearer liability allocation frameworks, while India must also confront its own forensic and evidentiary gaps if reforms are to succeed in practice. Ultimately, trust is the foundation of the FinTech ecosystem. If the law fails to evolve, every unremedied phishing loss chips away at confidence. But by embedding fairness, transparency, and accountability into the system, India can ensure that digital finance continues to innovate safely and inclusively.

References

1. Press Information Bureau. Digital Payment Transactions Surge with Over 18,000 Crore Transactions in 2024 25 (Mar. 11, 2025), 2025. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110405 (last visited Sept. 24, 2025).
2. Press Information Bureau. Advancing Cashless India (policy note / document) (Mar. 24, 2025) (noting the aim to reach nearly 20,000 crore UPI transactions in FY 2024-25), 2025. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/mar/doc2025324525401.pdf (last visited Sept. 24, 2025).
3. Reserve Bank of India. Annual Report 2024-25 (May 29, 2025) (UPI accounted for ~48.5% of world real-time payment volume, FY25),2025. https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT202425DA4AE08189C848C8846718B080F2A0A9.PDF (last visited Sept. 24, 2025).
4. FBI, IC3. 2024 IC3 Annual Report (Dec. 3, 2024) (IC3 received 859,532 complaints in 2024 and reported $16.6 billion in losses), 2024. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last visited Sept. 24, 2025).
5. Information Technology Act, No. 21 of 2000, Sec. 66C–66D (India); Reserve Bank of India. Customer Protection-Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (July 6, 2017), 2017. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI77D2F24BD1B98A4372829BF420EDC2E39.PDF (last visited Sept. 24, 2025); Consumer Protection Act, No. 35 of 2019, Sec. 2(47) (India).
6. Directive (EU) 2015/2366. Payment Services Directive (PSD2), 2015 O.J. (L 337) 35 (Strong Customer Authentication); see Payment Systems Regulator (UK). Authorised Push Payment (APP) Scams materials, 2023. https://www.psr.org.uk (last visited Sept. 24, 2025); Electronic Fund Transfer Act,15 U.S.C. Sec. 1693; 12 C.F.R. Sec. 1005 (Regulation E) (U.S.).
7. Payment Systems Regulator (UK). Authorised Push Payment (APP) Scams: Reimbursement Model,2023. https://www.psr.org.uk/our-work/app-scams/ (last visited Sept. 25, 2025).
8. Unified Payments Interface Circulars, NPCI, https://www.npci.org.in/what-we-do/upi/circular (last visited Sept. 24, 2025).
9. US. Department of Justice. United States Files Civil Forfeiture Complaint Against $225M in Funds Involved in Cryptocurrency Investment Fraud Money Laundering (June 18, 2025), 2025. https://www.justice.gov/opa/pr/united-states-files-civil-forfeiture-complaint-against-225m-funds-involvedcryptocurrency (last visited Sept. 24, 2025).
10. Information Technology Act, No. 21 of 2000, Sec. 66C, 66D (India), available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Sept. 24, 2025).
11. Consumer Protection Act, No. 35 of 2019, Sec. 2(47) (India), available at https://ncdrc.nic.in/bare_acts/CPA2019.pdf (last visited Sept. 24, 2025).
12. Reserve Bank of India. Customer Protection - Limiting Liability in Unauthorized Electronic Banking Transactions (July 6, 2017), 2017. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI77D2F24BD1B98A4372829BF420EDC2E39.PDF (last visited Sept. 24, 2025).
13. Lending Standards Board. Contingent Reimbursement Model (CRM) Code, and Payment Systems Regulator materials on APP scams (UK), 2023. https://www.lendingstandardsboard.org.uk/crm-code/ and https://www.psr.org.uk/our-work/app-scams/ (last visited Sept. 24, 2025).
14. Information Technology Act, No. 21 of 2000, Sec. 66C–66D (India), available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Sept. 25, 2025).
15. Consumer Protection Act, No. 35 of 2019, Sec. 2(47) (India), available at https://ncdrc.nic.in/bare_acts/CPA2019.pdf (last visited Sept. 25, 2025).
16. Reserve Bank of India. Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (July 6, 2017), 2017. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI77D2F24BD1B98A4372829BF420EDC2E39.PDF (last visited Sept. 25, 2025).
17. Directive (EU) 2015/2366. Payment Services Directive (PSD2), 2015 O.J. (L 337) 35 (Strong Customer Authentication), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 (last visited Sept. 25, 2025).
18. Lending Standards Board. Contingent Reimbursement Model (CRM) Code,2023. https://www.lendingstandardsboard.org.uk/crm-code/ (last visited Sept. 25, 2025).
19. Payment Systems Regulator (PSR). APP Scams Reimbursement (2023–25), 2025.

https://www.psr.org.uk/our-work/app-scams/ (last visited Sept. 25, 2025).
20. Electronic Fund Transfer Act,15 U.S.C. Sec. 1693 (1978), available at https://www.govinfo.gov/content/pkg/USCODE-2022-title15/pdf/USCODE-2022-title15-chap41-subchapVI.pdf (last visited Sept. 25, 2025).
21. 12 C.F.R. Sec. 1005 (Regulation E), available at https://www.consumerfinance.gov/rules-policy/regulations/1005/ (last visited Sept. 25, 2025).
22. "Bank fraud value trebles in FY25 despite drop in cases: RBI Annual report." New Indian Express, 2025. https://www.newindianexpress.com/business/2025/May/29/bank-fraud-value-trebles-in-fy25-despite-drop-in-cases-rbi-annual-report (last visited Sept. 24, 2025).
23. "Bank fraud cases fell in FY25, amount rose threefold to ₹36,014 cr: RBI." Business Standard, 2025. https://www.business-standard.com/finance/news/bank-fraud-amount-triples-in-fy25-despite-drop-in-number-of-cases-rbi-125052900696_1.html (last visited Sept. 24, 2025).
24. *State Bank of India v. Suresh Babulal Vora*, Complaint No. 135 of 2020 (Gujarat State Consumer Disputes Redressal Comm'n Aug. 12, 2022).
25. Punjab Nat'l Bank v. Leader Valves Ltd., Revision Petition No. 447 of 2017 (Nat'l Consumer Disputes Redressal Comm'n May 11, 2018).
26. FIU-IND. AML & CFT Guidelines for Reporting Entities (Mar. 10, 2023), 2023. https://fiuindia.gov.in/pdfs/AML_legislation/AMLCFTguidelines10032023.pdf (last visited Sept. 24, 2025).
27. "1 in 5 UPI users faced fraud; 51% victims didn't report, reveals survey." Business Standard, 2025. https://www.business-standard.com/finance/news/upi-transaction-fraud-india-survey-one-in-five-users-hit-localcircles-125062601141_1.html (last visited Sept. 24, 2025).
28. U.S. Department of Justice. United States v. $225M in Cryptocurrency Involved in Investment Fraud (June 18, 2025), 2025. https://www.justice.gov/opa/pr/united-states-files-civil-forfeiture-complaint-against-225m-funds-involved-cryptocurrency (last visited Sept. 25, 2025).
29. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023 (Sept. 2023), 2023. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 (last visited Sept. 25, 2025).