Page 3085 - 3098

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Emerging Trends and Techniques in Money-Extraction Cybercrimes: An Interdisciplinary Analysis of India's Digital Payment Vulnerabilities

PRANJUL BARCHE*

ABSTRACT

India's rapid digital financial transformation has fundamentally restructured the architecture of retail payments, financial inclusion, and banking operations. The expansion of real-time digital payment infrastructure, particularly through the Unified Payments Interface (UPI), Aadhaar-linked authentication systems, and mobile banking, has simultaneously enabled a new class of cyber-enabled financial offences that rely not on system intrusion or technical breach but on deception-driven fund extraction. This paper conceptualizes these offences as "money-extraction cybercrimes," defined as digitally mediated financial frauds in which victims voluntarily authorize transfers under psychological manipulation, impersonation, or synthetic technological simulation. Drawing upon criminology, behavioral economics, cybersecurity engineering, financial regulation, and Indian statutory law, the study develops an interdisciplinary analytical framework to examine emerging scam typologies, including digital arrest frauds, AI-enabled voice cloning, deepfake impersonation, SIM-swap attacks, mule account networks, and hybrid romance-investment schemes. Using data trends from the National Crime Records Bureau, the Reserve Bank of India, and the Indian Cyber Crime Coordination Centre, the paper identifies structural vulnerabilities within India's digital financial ecosystem. The study critically evaluates the adequacy of the Information Technology Act, 2000 (read with its 2008 amendment), the Bharatiya Nyaya Sanhita, 2023, the Reserve Bank of India's Digital Payment Security Controls, and customer liability frameworks, arguing that existing regulatory structures are calibrated primarily for unauthorized access scenarios and remain under-equipped to address deception-based voluntary transfers, especially those enhanced by artificial intelligence. The paper proposes a lifecycle-based intervention model integrating behavioral anomaly detection, telecom-bank coordination, real-time fund freezing mechanisms, regulatory clarification of liability standards, and AI authentication countermeasures, concluding that safeguarding India's digital payment

* Author is a Research Scholar at Maharashtra National Law University, Nagpur, Maharashtra, India.

 [ISSN 2581-5369]

infrastructure requires a coordinated socio-technical governance model bridging cybersecurity engineering, financial supervision, behavioral science, and criminal law.

Keywords: *Money-extraction cybercrime, Digital arrest fraud, Unified Payments Interface, Deepfake impersonation, Digital payment security, Customer liability.*

I. INTRODUCTION

India's digital public infrastructure has transformed its financial landscape at unprecedented speed. The Unified Payments Interface (UPI), introduced in April 2016 by the National Payments Corporation of India (NPCI), has emerged as the world's largest real-time retail payment system, processing 185.87 billion transactions in the financial year 2024-25 alone. The Reserve Bank of India (RBI) has repeatedly highlighted the scale, velocity, and systemic importance of digital payment growth in its annual and payment system reports.

The architecture of interoperable instant payments, Aadhaar-linked identity verification, and widespread smartphone penetration has enabled financial participation across rural and urban divides. Financial inclusion has expanded dramatically through Aadhaar-enabled payment systems, mobile banking platforms, direct benefit transfers, and QR-code-based merchant payments. The integration of identity, payments, and mobile connectivity within India's Digital Public Infrastructure framework is globally regarded as a model for scalable fintech innovation. Yet rapid digitization has not merely expanded opportunity; it has reconfigured risk. The same characteristics that make India's payment ecosystem efficient, namely speed, interoperability, and frictionless authentication, have also amplified the potential for exploitation.

Cybercrime in India has evolved accordingly. Early digital financial crimes were predominantly characterized by unauthorized access, malware deployment, phishing for credentials, or technical compromise of systems. Increasingly, however, financial cyber offences involve socially engineered deception in which victims themselves authorize fund transfers. The National Crime Records Bureau (NCRB) documented 65,893 cybercrime cases in 2022, rising to 82,967 cases in 2023, an increase of approximately 26 percent. RBI annual reports similarly indicate growing digital payment fraud incidents, with card-not-present transactions, remote banking channels, and mobile-based payment systems showing particular vulnerability.

This shift reflects a transformation in threat methodology. Rather than breaching technical perimeters, perpetrators exploit behavioral vulnerabilities. Victims are induced, through impersonation of law enforcement officers, fabricated regulatory threats, AI-generated voice cloning of relatives, or investment-based emotional manipulation, to voluntarily transfer funds.

 [ISSN 2581-5369]

In such cases, the payment infrastructure itself may operate exactly as designed. Authentication protocols are satisfied, credentials are valid, and transaction logs show no system intrusion, yet financial harm occurs. The exploited vector is not a software flaw but human cognition under conditions of psychological pressure.

This transformation challenges traditional legal and cybersecurity classifications. Existing regulatory frameworks are largely structured around "unauthorized access" or "system compromise." However, deception-induced voluntary transfers blur established boundaries between authorized and unauthorized transactions. The RBI's customer liability circular distinguishes between unauthorized electronic banking transactions and those attributable to customer negligence. In deception-based scams, determining the degree of negligence as against manipulation becomes legally complex. Similarly, penal statutes such as the Information Technology Act, 2000 (read with its 2008 amendment) and the Bharatiya Nyaya Sanhita, 2023 address cheating and computer-related offences, but their interpretive application to AI-enabled impersonation and cross-border digital scam syndicates raises doctrinal and evidentiary challenges.

The emergence of artificial intelligence tools further complicates the landscape. Generative AI technologies now enable realistic voice cloning and deepfake video impersonation using minimal publicly available data. The capacity to simulate trusted identities in real time erodes traditional verification cues and magnifies authority bias and emotional vulnerability. As India deepens its digital penetration across socio-economic strata, the scale of exposure correspondingly expands.

Against this backdrop, this paper introduces and analytically develops the concept of money-extraction cybercrime. The term refers to digitally mediated financial offences in which perpetrators induce victims to authorize electronic fund transfers through deception, impersonation, psychological manipulation, or synthetic technological simulation. By conceptualizing these offences as a distinct socio-technical category, the paper seeks to bridge gaps between cybersecurity engineering, behavioral science, financial regulation, and criminal law.

The study is guided by three central research questions. First, how has India's digital payment architecture altered the typology and mechanics of financial cybercrime? Second, to what extent do existing legal and regulatory frameworks adequately address deception-based voluntary transfers? Third, what interdisciplinary interventions, whether technical, behavioral, or regulatory, are necessary to mitigate money-extraction cybercrime in India?

 [ISSN 2581-5369]

Methodologically, the paper adopts a doctrinal analysis of statutory and regulatory instruments, an empirical examination of publicly available NCRB, RBI, and Indian Cyber Crime Coordination Centre (I4C) data, and a socio-technical analytical framework integrating criminological theory and behavioral economics. The objective is not merely descriptive but diagnostic, namely to identify structural vulnerabilities and propose integrated governance responses.

The remainder of this paper proceeds as follows. The next part surveys existing literature on financial cybercrime evolution and behavioral exploitation. The paper then develops the conceptual framework for defining money-extraction cybercrime, classifies emerging scam typologies in India, and analyzes technical architecture vulnerabilities within digital payment systems. It subsequently examines empirical trends, evaluates the adequacy of legal and regulatory mechanisms, and proposes an institutional liability mapping framework. The paper concludes by outlining the interdisciplinary policy reforms necessary to safeguard India's digital financial future. In doing so, the study argues that securing India's digital payment revolution requires moving beyond traditional cybersecurity paradigms toward an integrated socio-technical regulatory approach.

II. LITERATURE REVIEW

A. Evolution of financial cybercrime

Early cybercrime literature focused on unauthorized access, malware propagation, and data exfiltration. More recent scholarship, however, recognizes the rise of social engineering as a dominant threat vector. The *Verizon Data Breach Investigations Report* consistently identifies phishing and pretexting as primary initial access vectors in financial breaches globally.[1]

In the Indian context, academic discussion has largely concentrated on compliance with the Information Technology Act and its penal provisions, with limited integration of behavioral science or payment system architecture analysis. The emerging scholarship on money-extraction cybercrimes remains fragmented across disciplines, lacking a unified conceptual framework that bridges technical security, behavioral economics, and regulatory policy.

B. Routine activity theory and digital ecosystems

Routine activity theory posits that crime arises when a motivated offender encounters a suitable target in the absence of capable guardians. Real-time digital payment systems increase target availability while reducing temporal barriers to transaction completion. The theory's

[1] Verizon Business, *2025 Data Breach Investigations Report* (2025), https://www.verizon.com/business/resources/T1f9/reports/2025-dbir-data-breach-investigations-report.pdf.

 [ISSN 2581-5369]

applicability to cybercrime has been demonstrated in studies showing how digital environments create a convergence of offenders and victims across geographical boundaries, with guardianship functions distributed across technical systems rather than human monitors.[2]

C. Behavioral economics and authority bias

Behavioral research demonstrates that urgency, fear, and perceived authority impair rational decision-making. Daniel Kahneman's work on cognitive biases establishes that intuitive, fast thinking dominates under emotional stress, precisely the condition that scam narratives deliberately induce.[3] Authority bias, scarcity bias, and emotional triggers are systematically exploited in contemporary fraud schemes. The digital arrest phenomenon exemplifies this manipulation, with perpetrators impersonating law enforcement to trigger compliance responses rooted in deference to authority.

D. Artificial intelligence and synthetic impersonation

Generative AI technologies now enable voice cloning and deepfake video impersonation with minimal input data. Research indicates that current detection methods struggle with real-time synthetic media, particularly when audio and video are combined.[4] India-specific research on AI-enabled financial fraud remains limited, creating a scholarly gap that this paper addresses through empirical analysis of emerging scam typologies and regulatory responses.

III. CONCEPTUALIZING MONEY-EXTRACTION CYBERCRIME

This paper defines money-extraction cybercrime as a digitally mediated financial offence in which perpetrators employ deception, impersonation, psychological coercion, or synthetic technological simulation to induce the voluntary authorization of electronic fund transfers.

This definition distinguishes such crimes from "unauthorized access" under Section 43 of the Information Technology Act, 2000, where perpetrators bypass authentication mechanisms without the victim's knowledge. In money-extraction cybercrimes, the victim actively participates in the transaction, albeit under manipulated conditions. The authorization is technically valid but ethically and legally compromised through deception.[5]

The conceptual framework identifies four constitutive elements. First, digital mediation: the offence occurs through electronic payment systems, telecommunications, or internet-based

[2] Eric Rutger Leukfeldt & Majid Yar, *Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis*, 37 DEVIANT BEHAV. 263 (2016).
[3] Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263 (1979).
[4] Maura R. Grossman et al., *The GPTJudge: Justice in a Generative AI World*, 23 DUKE L. & TECH. REV. 1 (2023).
[5] Leukfeldt & Yar, *supra* note 2, at 271.

 [ISSN 2581-5369]

platforms. Second, deceptive inducement: perpetrators employ misrepresentation, impersonation, or psychological manipulation. Third, voluntary authorization: victims themselves initiate or approve fund transfers through legitimate authentication protocols. Fourth, financial extraction: the objective is monetary gain through the transfer of funds rather than data theft or system damage.

This framework enables analysis of offences that fall between the traditional categories of cybercrime and financial fraud, requiring interdisciplinary responses that technical security measures alone cannot provide.

IV. Emerging typologies in India

The following table sets out a typology of money-extraction cybercrimes.

Scam Type	Technology Used	Psychological Lever	Payment Channel
Digital Arrest	Video spoofing, forged IDs	Authority fear	UPI/IMPS
AI Voice Clone	Generative AI	Emotional panic	Mobile wallets
SIM-Swap	Telecom manipulation	Confusion	Net banking
Romance-Investment	Social media grooming	Trust/greed	Crypto/UPI
Mule Networks	Layered transfers	Obfuscation	Multiple accounts

A. Digital arrest fraud

Digital arrest fraud represents the most rapidly growing money-extraction cybercrime category in India. According to data from the Indian Cyber Crime Coordination Centre, cases surged from 39,925 in 2022 to 123,672 in 2024, an increase of approximately 210 percent, while financial losses rose from ₹91 crore to ₹1,918 crore, representing an increase of approximately 2,007 percent.[6]

The modus operandi involves fraudsters impersonating law enforcement officers from agencies such as the Central Bureau of Investigation and the Narcotics Control Bureau, or customs officials. Victims receive calls alleging involvement in serious crimes such as money laundering, drug trafficking, or financial fraud, backed by fabricated First Information Report numbers, arrest warrants, and official-looking documents transmitted via WhatsApp or email. The psychological escalation involves video calls in which perpetrators wear police uniforms, display forged credentials, and conduct mock interrogations.

[6] *Digital Arrest Cases Surge in India, I4C Data Shows*, Indian Express, https://indianexpress.com/article/technology/tech-news-technology/digital-arrest-cases-rise-india-i4c-data-9578423/ (last visited Apr. 20, 2026).

The innovation lies in the "digital custody" concept. Victims are instructed to remain under continuous video surveillance, forbidden from contacting family or leaving their location, creating conditions of isolation and psychological domination. The "arrest" is presented as avoidable through immediate payment of "verification fees," "court bonds," or "settlement amounts." High-profile victims have included S.P. Oswal, the textile magnate who lost ₹7 crore over two days;[7] Dr. Ruchika Tandon, a neurology professor defrauded of ₹2.81 crore;[8] and a retired senior police officer who attempted to take his own life after losing over ₹8 crore.[9]

Geographic distribution data reveals concentrated impact in major economic hubs. Maharashtra led with approximately 303,000 total cybercrime complaints in 2024, followed by Uttar Pradesh at approximately 301,000. Karnataka recorded 641 digital arrest cases with losses of ₹109 crore, with Bengaluru alone accounting for 480 cases and ₹42.4 crore in losses.[10]

I4C analysis indicates that 45 to 46 percent of digital arrest operations originate from Southeast Asian countries, primarily Cambodia, Myanmar, Laos, Thailand, and Vietnam, often from call centres housed within foreign-owned casino compounds. A further 30 to 40 percent of criminal activities have been traced to operatives within India.

B. AI-enabled voice cloning

Generative AI tools now replicate vocal patterns from publicly available audio samples as short as 30 seconds. Victims receive emergency calls from impersonated relatives requesting urgent financial assistance. The technology has advanced to real-time voice cloning during live calls, enabling dynamic conversation rather than pre-recorded messages.

In Kerala, a 73-year-old man lost ₹40,000 following a WhatsApp deepfake call that appeared to be from his friend, pleading for urgent help from Dubai.[11] A McAfee survey in November

[7] *Ludhiana: How Padma Awardee Vardhman Group's S.P. Oswal Lost Rs 7 Crore in Online Scam*, ECON. TIMES, https://economictimes.indiatimes.com/news/india/ludhiana-how-padma-awardee-vardhman-groups-sp-oswal-lost-rs-7-crore-in-online-scam/articleshow/113813450.cms (last visited Apr. 20, 2026).

[8] *PGI Doctor Scammed of ₹2.81 Crore in Digital Arrest Fraud*, TIMES OF INDIA, https://timesofindia.indiatimes.com/city/lucknow/pgi-doctor-scammed-of-281-crore-in-digital-arrest-fraud/articleshow/112536972.cms (last visited Apr. 20, 2026).

[9] *Retd IPS Officer Tries to End Life After Losing Rs 8 Crore to Cyber Swindlers*, HINDUSTAN TIMES, https://www.hindustantimes.com/india-news/retd-ips-officer-tries-to-end-life-after-losing-rs-8-crore-to-cyber-swindlers-101766443619592.html (last visited Apr. 20, 2026).

[10] Frank on Fraud, *Digital Arrest Scams Explained* (2026), https://frankonfraud.com/wp-content/uploads/2026/01/Digital-Arrest-Scams-Explained.pdf.

[11] *Deepfake Scammers Trick Indian Man into Transferring Money; Police Investigating Multi-Million Rupee Scam*, HINDUSTAN TIMES, https://www.hindustantimes.com/india-news/deepfake-scammers-trick-indian-man-into-transferring-money-police-investigating-multi-million-rupee-scam-101689622291654.html (last visited Apr. 20, 2026).

 [ISSN 2581-5369]

2024 found that 75 percent of Indians had seen deepfake content in the preceding year, and 45 percent reported knowing someone who had been duped by deepfake fraud.[12]

The psychological leverage exploits familial bonds and emergency response instincts. The "grandparent scam" variant specifically targets elderly individuals with fabricated scenarios of accidents, arrests, or medical emergencies affecting grandchildren. The urgency precludes verification, and the familiar voice eliminates suspicion.

C. SIM-swap attacks

SIM-swap fraud involves the unauthorized issuance of duplicate SIM cards, enabling the interception of one-time passwords (OTPs). Perpetrators gather personal information through phishing or data breaches, then convince telecom customer service representatives to port the victim's number to a new SIM. Once activated, all OTPs and banking alerts route to the attacker's device.[13]

The Department of Telecommunications has attempted to address this through SIM binding requirements, mandating that mobile banking applications remain linked to the original SIM card. However, regulatory oversight gaps persist, particularly regarding verification protocols at retail points of sale and customer service centres.

D. Romance-investment scams

Hybrid schemes combine emotional manipulation through dating platforms with fraudulent investment opportunities. Perpetrators establish romantic relationships over weeks or months before introducing "exclusive" cryptocurrency or forex trading platforms. Victims transfer funds to controlled accounts, with initial "profits" displayed to encourage larger investments. The scheme collapses when victims attempt withdrawals or the relationship terminates.[14]

These scams exploit both trust and greed, with the emotional component delaying recognition of financial red flags. The use of cryptocurrency complicates recovery efforts, as transactions are irreversible and wallet addresses provide limited identification.[15]

---

[12] McAfee, *Press Release* (Nov. 21, 2024), https://www.mcafee.com/en-in/consumer-corporate/newsroom/press-releases/2024/20241121.html.

[13] Nathanael Andrews, *Can I Get Your Digits?: Illegal Acquisition of Wireless Phone Numbers for SIM-Swap Attacks and Wireless Provider Liability*, 16 NW. J. TECH. & INTELL. PROP. 79 (2018).

[14] Shalini Nataraj-Hansen, *Blaming Victims of Online Romance and Investment Frauds: An Analysis of Two Theoretical Perspectives* (2024) (Ph.D. dissertation, Queensland University of Technology).

[15] David Adam Friedman, *Impostor Scams*, 54 U. MICH. J.L. REFORM 611 (2021).

 [ISSN 2581-5369]

E. Mule account networks

Mule accounts serve as intermediaries in financial crime, receiving the proceeds of fraud before transferring funds, often across borders, to ultimate beneficiaries. The Reserve Bank of India estimates that organized fraud networks utilize thousands of such accounts, often opened by unwitting individuals recruited through fake job offers or romance scams.[16]

Traditional fraud detection systems rely on static, rule-based models that flag accounts based on fixed criteria. However, these systems generate high false positives and cannot adapt swiftly to evolving criminal behavior.

V. TECHNICAL ARCHITECTURE AND SYSTEMIC VULNERABILITIES

India's digital payment systems rely on multi-factor authentication, OTP verification, and device binding mechanisms. However, several structural vulnerabilities persist that enable money-extraction cybercrimes.

A. Real-time settlement irreversibility

UPI transactions settle instantly, reducing recovery windows. Unlike card payments, where chargeback mechanisms exist, authorized UPI transfers are final. The "golden hour" for freezing funds requires immediate reporting, yet victims often realize that a fraud has occurred only after significant delays.[17]

B. OTP reliance

OTP-based authentication shifts the security burden to end users. When users manually enter OTPs, fraud may be attributed to customer error, limiting institutional liability and the motivation for stronger controls. OTP-only approaches cannot detect SIM-swap or cloning attacks, as wrongdoers still receive OTPs and appear legitimate.[18]

C. Interoperability risk propagation

The interconnectivity of the payment ecosystem allows rapid fund dispersion across multiple accounts and institutions. A single fraudulent transfer can cascade through mule networks within minutes, complicating tracing and freezing efforts.[19]

---

[16] Udom Netrattanagul, *Guarding the Financial System: Strengthening IT Governance to Combat Mule Accounts*, ISACA J., vol. 4 (2025).

[17] Morten L. Bech & Bart Hobijn, *Technology Diffusion Within Central Banking: The Case of Real-Time Gross Settlement* (Fed. Rsrv. Bank of N.Y., Staff Report No. 260, 2006).

[18] Burhan Ul Islam Khan et al., *Offline OTP Based Solution for Secure Internet Banking Access*, in 2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e) (2018).

[19] Massimo Migliorini et al., *Data Interoperability for Disaster Risk Reduction in Europe*, 28 DISASTER PREVENTION & MGMT.: INT'L J. 804 (2019).

 [ISSN 2581-5369]

D. Behavioral blind spots in fraud detection

Many fraud monitoring systems focus on anomalous device signatures or transaction patterns rather than indicators of psychological coercion. A victim authorizing transfers under duress generates technical signatures identical to those of legitimate transactions, thereby bypassing automated detection.[20]

VI. Empirical trends in India

NCRB data indicates consistent year-on-year growth in cybercrime cases. From 44,735 cases in 2019, registered cybercrimes increased to 50,035 in 2020, 52,974 in 2021, and 65,893 in 2022. The 2023 data show further acceleration to 82,967 cases. However, conviction rates remain alarmingly low, at 0.82 percent in 2019, 2.22 percent in 2020, and 0.93 percent in 2021, indicating systemic inefficiencies in investigation and prosecution.[21]

Digital payment fraud specifically has grown at an even faster rate. According to RBI data, digital payment fraud cases increased from 119,699 in 2020-21 to 1,457,000 in 2023-24, a compound annual growth rate of approximately 130 percent. The amount involved rose from ₹290 crore to ₹2,604 crore during the same period, with a compound annual growth rate of approximately 108 percent.[22]

The RBI Annual Report 2023-24 reveals that the total number of fraud cases reported jumped from 13,564 in 2022-23 to 36,075 in 2023-24, an increase of approximately 165 percent. While the amount involved in frauds fell by approximately 47 percent to ₹13,930 crore, the sheer number of frauds affecting the banking system remains staggering.[23]

For private sector banks, frauds have occurred predominantly in the category of digital payments (card and internet), while for public sector banks, credit frauds continue to be most dominant. The quantum of frauds arising from credit cards or internet banking increased significantly, from 0.1 percent in 2018-19 to 10.5 percent in 2023-24.

The Indian Computer Emergency Response Team (CERT-In) has issued advisories repeatedly warning of phishing, vishing, and AI-enabled fraud techniques. However, the dissemination of

[20] Mark Edmonds, Kate B. Sorensen & Matthew A. Stallings, *The Invisible Fraud: The Impact of Inattentional Blindness on Auditor Fraud Detection*, 6 J. Forensic Acct. Rsch. 57 (2021).
[21] Nat'l Crime Recs. Bureau, Ministry of Home Affairs, Gov't of India, *Crime in India* tbl. 14A.2 (2019-2023), https://ncrb.gov.in/crime-india.
[22] Reserve Bank of India, *Annual Report 2023-24* 248-52 (2024), https://rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1378.
[23] Reserve Bank of India, *Annual Report 2023-24* 248-52 (2024), https://rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1378.

 [ISSN 2581-5369]

advisories does not automatically translate into behavioral change at the population scale required.

These trends demonstrate a migration from technical exploitation toward cognitive manipulation. The average loss per digital arrest victim rose from approximately ₹22,826 in 2022 to ₹1,56,502 in 2024, indicating increasingly sophisticated targeting of high-net-worth individuals.

VII. LEGAL AND REGULATORY FRAMEWORK

A. Information Technology Act, 2000

Sections 43 and 66 address unauthorized access and computer-related offences. However, a voluntary transfer made under deception may fall outside the strict definition of "unauthorized access." Section 66C (identity theft) and Section 66D (cheating by personation) apply to impersonation elements, but the evidentiary requirements for electronic records, together with the involvement of cross-border perpetrators, create enforcement challenges.[24]

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS) incorporates cheating (Sections 318 to 319) and impersonation provisions applicable to financial scams. Section 111 includes cybercrimes within the definition of organized crime when committed as part of syndicate activity, thereby enabling the prosecution of actors, financiers, and facilitators.[25]

However, the BNS does not contain a chapter exclusively titled "Cybercrimes." Instead, offences traditionally viewed as cybercrimes are prosecuted under general provisions when conducted through digital means. Digital-specific evidentiary complexities, such as proving criminal intent in AI-mediated impersonation or establishing jurisdiction over foreign-operated scam centres, remain unresolved.

C. RBI customer liability framework

The RBI's circular of 6 July 2017 on customer liability distinguishes between unauthorized electronic banking transactions and customer negligence. Zero liability applies where fraud occurs due to bank negligence or third-party breaches reported within three working days.

[24] The Information Technology Act, 2000, §§ 43, 66, 66C, 66D, No. 21, Acts of Parliament, 2000 (India), https://www.indiacode.nic.in/handle/123456789/1999.

[25] The Bharatiya Nyaya Sanhita, 2023, §§ 111, 318-319, No. 45, Acts of Parliament, 2023 (India), https://www.indiacode.nic.in/handle/123456789/20062.

 [ISSN 2581-5369]

Limited liability, capped at between ₹5,000 and ₹25,000 depending on account type, applies for delays of four to seven days. Beyond seven days, liability follows bank policy.[26]

Deception-induced transfers often create ambiguity in liability determination. The bank bears the burden of proving customer negligence, yet the psychological manipulation involved in money-extraction cybercrimes complicates categorization. Victims who voluntarily share OTPs under duress may technically appear negligent while in fact being exploited.

D. Digital payment security controls

The RBI's Master Direction on Digital Payment Security Controls, updated in 2024, mandates risk-based monitoring, board-approved security policies, and fraud detection systems. The Master Directions of 30 July 2024 on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators establish governance frameworks, baseline security measures, and implementation timelines (large operators by 1 April 2025; medium operators by 1 April 2026; small operators by 1 April 2028).[27]

Key requirements include 12-hour cooling periods for changes to registered mobile numbers, secure communication protocols, and multi-factor authentication. Yet AI-enabled impersonation presents new detection challenges that existing controls do not fully address.

VIII. LIABILITY MAPPING

The following table sets out an institutional responsibility matrix.

Stage	Actor	Regulatory Basis	Risk
SIM issuance	Telecom provider	DoT/Telecom norms	Identity misuse
Account onboarding	Bank	KYC/AML norms	Mule accounts
Transaction processing	Bank/NPCI	RBI DPS Controls	Real-time loss
Post-fraud	Bank/Police	Customer Liability Circular	Recovery gaps

Current liability frameworks distribute responsibility across institutions without ensuring seamless coordination. Telecom providers bear limited liability for SIM-swap fraud; banks dispute negligence determinations; and law enforcement faces jurisdictional barriers in cross-border operations. The victim navigates this fragmented landscape while facing statutory limitation periods and evidentiary burdens.

[26] Reserve Bank of India, *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 (July 6, 2017), https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11027.

[27] Reserve Bank of India, *Master Direction on Digital Payment Security Controls* (2024).

IX. INTERDISCIPLINARY DISCUSSION

Money-extraction cybercrime exposes a regulatory blind spot. Traditional cybersecurity models prioritize perimeter defence and system hardening. However, deception-based crimes target human cognition within secure perimeters. The "human firewall" concept, which relies on user awareness and vigilance, proves insufficient against sophisticated psychological manipulation and AI-generated synthetic media.

An effective response requires several integrated approaches. As regards cybersecurity engineering integration, fraud detection systems must incorporate behavioral indicators of coercion, not merely technical anomalies. Device binding, biometric liveness detection, and transaction pattern analysis should identify high-risk scenarios requiring stepped-up authentication.[28]

As regards behavioral economics integration, public awareness must move beyond generic warnings toward cognitive bias inoculation. Training individuals to recognize authority bias, urgency manipulation, and emotional exploitation provides psychological defences against social engineering.[29]

As regards regulatory clarification, the RBI must clarify liability standards for deception-induced voluntary transfers. The current negligence framework inadequately addresses manipulation scenarios in which victims technically authorize transactions while being psychologically compromised.[30] As regards telecom-bank coordination, the prevention of SIM-swap fraud requires stricter telecom know-your-customer verification, real-time notification of number porting attempts, and shared fraud intelligence between sectors.

As regards AI countermeasures, digital authentication must move toward biometric liveness detection and AI-generated content identification. The IndiaAI Mission's funding of deepfake detection projects through the Indian Institutes of Technology represents an initial step toward indigenous technical capabilities.[31]

---

[28] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* 212-19 (2000).

[29] Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* 37-45 (2d ed. 2008).

[30] Reserve Bank of India, *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 (July 6, 2017), https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11027.

[31] Indian Institute of Technology Jodhpur, *Deepfake Detection and AI Security Research Initiatives*.

 [ISSN 2581-5369]

X. POLICY RECOMMENDATIONS

First, statutory recognition of AI-enabled impersonation: the Information Technology Act should be amended to specifically criminalize the use of synthetic media for financial fraud, with enhanced penalties for organized operations.

Second, a real-time transaction reversal escrow: a regulatory framework should be established permitting provisional transaction holds when behavioral anomaly detection triggers alerts, pending victim confirmation.

Third, an RBI circular clarifying the burden of proof: specific guidance should be issued on liability determination for deception-based voluntary transfers, establishing presumptions favouring victims where psychological coercion is evidenced.

Fourth, a CERT-In advisory on deepfake financial fraud: financial institutions should be mandated to implement voice and video verification protocols for high-value transactions, with standardized detection tool integration.

Fifth, a national awareness campaign targeting authority bias: targeted educational content should be developed addressing the specific psychological vulnerabilities exploited in digital arrest and AI-impersonation scams, delivered through banking channels and telecom alerts.

XI. CONCLUSION

India's digital payment revolution has reshaped economic participation, with UPI processing 185.87 billion transactions in the financial year 2024-25 and digital payments comprising 99.7 percent of transaction volume in 2024. However, the evolution of money-extraction cybercrime demonstrates that technological security alone is insufficient. Deception-based voluntary transfers expose regulatory and cognitive vulnerabilities that require interdisciplinary responses.

The transformation from technical exploitation to psychological manipulation challenges existing legal categories calibrated for unauthorized access. The framework of the Information Technology Act and the general provisions of the Bharatiya Nyaya Sanhita struggle to address AI-enabled impersonation, cross-border syndicates, and the fundamental ambiguity of "authorized" transactions induced through deception.

The future of financial cybersecurity in India depends not merely on stronger encryption but on integrated socio-technical governance, combining engineering safeguards, behavioral insight, telecom oversight, and legal adaptation. The RBI's initiatives, the Master Directions on Digital Payment Security Controls, and Project Nexus for cross-border payments represent

 [ISSN 2581-5369]