International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 12-08-2025, Accepted: 11-09-2025, Published: 26-09-2025
Volume 11, Issue 9, 2025, Page No. 81-89

Hook, line & launder: Tracing phishing frauds and money-laundering networks in India

Jasmine Sharma
Advocate, Practising in Delhi and West Bengal District Courts, Delhi, India

Abstract
India's unprecedented digital payments boom, led by the Unified Payments Interface (UPI), has transformed financial inclusion while simultaneously exposing users to new-age cyber threats. Among these, phishing a tactic exploiting human vulnerability and its subsequent integration into sophisticated money laundering chains pose one of the most pressing challenges to India's digital economy. This paper undertakes a comprehensive, data-driven examination of phishing-enabled laundering networks in India, contextualised within evolving legal, technological, and enforcement landscapes.
Through the analysis of real-life case studies, including the recent "digital arrest" scam in Ahmedabad and UPI-linked cross-border laundering via crypto exchanges, the study reveals structural weaknesses in regulatory coordination, technological safeguards, and public awareness. By integrating insights from the Prevention of Money Laundering Act, 2002 (PMLA), Information Technology Act, 2000, and emerging frameworks such as the RBI's Digital Payments Intelligence Platform, this research identifies critical gaps in the detection, investigation, and prosecution of phishing-related laundering offences.
The paper proposes a National Phishing and Laundering Response Framework (NPLRF) to unify stakeholders, leverage AI-powered predictive analytics, and enhance cross-border cooperation, while embedding cyber literacy as a national priority. It argues for a paradigm shift from reactive enforcement to proactive prevention, ultimately advocating for a resilient digital trust architecture. This research contributes to academic discourse, policy formulation, and law enforcement strategy, offering holistic solutions to balance financial innovation with systemic security in India's evolving fintech ecosystem.

Keywords: Phishing, money laundering, upi fraud, cybercrime, pmla, digital payments security, ai-based fraud detection

Introduction

1. The Rising Sophistication of Phishing and Laundering Networks

Unlike traditional fraud schemes, modern phishing in India has evolved into multi-layered criminal ecosystems that operate with striking precision. Fraudsters are no longer isolated hackers; they now form coordinated networks involving technology suppliers, call-centre operatives, money mules, crypto-wallet handlers, and international laundering syndicates. The "digital arrest" scams epitomise this sophistication. In September 2025, a 78-year-old retired banker from Ahmedabad lost ₹39 lakh after receiving a fake video call where cybercriminals posed as Mumbai Police officers, complete with cloned voices and forged IDs, coercing him into transferring funds under the threat of prosecution [1]. These cases are not isolated; they form part of scalable phishing-as-a-service (PhaaS) models, where phishing kits, fake UPI interfaces, deepfake video templates, and even mule accounts are rented on the dark web for as little as $50 per week [2].

The situation worsens when laundering pipelines integrate seamlessly with phishing scams. Once stolen, the funds are routed through layered UPI transfers, dormant Jan Dhan accounts, crypto wallets, and offshore exchanges [3]. In December 2023, the Financial Intelligence Unit (FIU) issued show-cause notices to nine offshore crypto exchanges, including Binance and KuCoin, for facilitating laundering linked to phishing operations [4]. These networks exploit regulatory blind spots: UPI's instantaneous transfers, combined with limited cross-border KYC, make it nearly impossible to reverse fraudulent transactions. Adding complexity, phishing campaigns increasingly involve foreign-based command centres for example, multiple arrests in 2024 revealed syndicates operating from Cambodia and Dubai, orchestrating scams targeting Indian citizens [5]. What emerges is a globalised fraud economy, where domestic victims' losses fuel transnational laundering networks beyond India's direct jurisdiction.

2. The Legal and Institutional Challenge

India's legal response architecture has struggled to keep pace with the evolving threat landscape. While frameworks like the Information Technology Act, 2000, the Indian Penal Code (IPC) provisions on cheating, and the Prevention of Money Laundering Act, 2002 (PMLA) theoretically cover phishing-related laundering, they are often fragmented and reactive [6]. For example, under the PMLA, enforcement agencies require a predicate offence before acting against laundering [7]. This procedural dependency frequently delays intervention at critical stages when stolen funds are rapidly layered and moved offshore. A recent Supreme Court observation labelled this "a parasitic structure that allows laundering chains to survive longer than necessary," urging Parliament to rethink predicate dependencies in cyber-enabled laundering offences [8]. Moreover, enforcement coordination remains limited. CERT-In, RBI, NPCI, FIU, and state cybercrime cells operate in silos, resulting in delayed responses and fragmented intelligence sharing. Despite the RBI's announcement of a Digital Payments Intelligence Platform (DPIP) in 2024 to centralise real-time fraud detection [9], the absence of statutory compulsion for banks, payment apps, and crypto exchanges to integrate has slowed implementation. Meanwhile, public awareness remains alarmingly low: a 2025 Fortune India survey found that 1 in 5 UPI users experienced fraud, yet 51% of victims

never reported incidents, fearing prolonged police procedures or reputational harm [10]. The gap between policy ambition and ground-level preparedness enables phishing syndicates to scale faster than regulatory responses. This evolving threat underscores the urgent need for integrated reforms: a unified digital fraud law, an AI-driven real-time risk assessment system, and cross-border enforcement treaties targeting laundering chains. Without these systemic changes, India risks becoming not just a hotspot for phishing victims but also an unwitting node in global laundering economies. This paper, therefore, argues for a paradigm shift from fragmented, post-facto investigations to predictive, collaborative, and people-centric models laying the the foundation for a resilient digital trust infrastructure.

Chapter 2: From Hook to Launder: Anatomy of A Scam

The anatomy of a phishing-induced fraud in India can be likened to a tragic yet ingenious drama: the bait is cast, the victim takes the hook, blood invariably flows, and the laundering network washes it clean. In this chapter, we unravel this sequence step by step shedding light on how digitally stolen rupees voyage through mule accounts, crypto channels, shell structures, and foreign banking rails before emerging "clean." The goal is to depict not just a process but a landscape where law, psychology, and technology collide.

1. The Bait: Crafting the Phishing (The Hook)

The attack often begins with what appears benign an SMS, email, or WhatsApp message. It could masquerade as a government notice, a covid-19 aid link, or a court order, launching a sense of urgency that short-circuits rational judgment [14]. A classic example: a CERT-In advisory recounts how phishers may impersonate official email IDs like ncov2019@gov.in, inviting recipients to click on "free COVID-19 testing" links only to land on sophisticated yet bogus websites that harvest their credentials [10]. Alternatively, more personal tactics have emerged. In one scheme, scammers impersonated pension authorities, citing actual Aadhaar numbers and PPO details before coercing senior citizens into sharing OTPs quickly draining their pension accounts [20]. These psychological triggers pressure tactics, authoritative impersonation, and personalization are far more impactful than the technical exploits themselves.

2. The Bite: Execution of the Fraud (The Bleed)

Once the victim complies sharing credentials, clicking a link, or transferring funds the theft happens almost instantly, especially on rails like UPI or mobile banking. The funds evaporate from the victim's account within moments, feeding the next stage of the laundering pipeline. The question that then emerges electric in its urgency is where do the funds go, so fast? This leads us to the execution phase: dispatching the proceeds through layers designed to obscure, confuse, and eventually absolve.

3. The Bleed: Mule Accounts (Primary Layering)

In many schemes, the stolen funds are rapidly moved into mule accounts bank accounts held by unwitting individuals or paid runners. The central role of mule accounts in laundering operations has become impossible to ignore. In one major case involving chartered accountants (CAs), company secretaries, and crypto traders, the Enforcement Directorate (ED) uncovered more than 5,000 mule bank accounts used to siphon off ₹640 crore [11]. Another investigative blitz revealed that as many as 8.5 lakh mule accounts had been opened across 700 bank branches via procedural lapses bank staff ignored KYC norms, skipped due diligence, or turned a blind eye to suspicious alerts [12]. Given the scale, states are now reacting: Haryana [13] identified 91 bank branches linked to mule-account activity, and Odisha [14] has urged banks to block mule accounts proactively. These accounts are the first laundering layer invisible to victims, but glaring to investigators once patterns emerge.

4. The Wash: Crypto, Payment Platforms & Cross-Border Channels

Once proceeds are pooled into mule accounts, laundering often shifts to crypto platforms or digital payment networks. In the aforementioned ₹640 crore case, funds were uploaded onto PYYPL a UAE-based payment platform and part of the money was withdrawn in cash in Dubai using Indian-issued cards [15]. This pairing of mule accounts and crypto gateways allows swift layering and obfuscation. Crypto's anonymity and cross-jurisdictional reach make it ideal: once converted into USDT or similar tokens, the path back to law enforcement becomes increasingly obscure especially when hosted offshore or mixed across wallets.

5. The Dry: Structural Integration (Shells, Real Estate & Offshore Vehicles)

With the money "washed," criminals turn to integration: embedding proceeds into legitimate-looking assets. Often, they rely on shell companies, real estate, or foreign investments to bury the origin. Though not always explicitly tied to phishing, ED raids have exposed how laundering often ends in structured assets. A recent enforcement action uncovered shell companies funneling money into foreign properties Dubai, Singapore, Cyprus under layers of ownership that hide beneficiaries [16]. Even in property-level laundering, tiny channels like forged documentation, offshore shell entities, and nominee structures build a barrier between the money and its illicit origins.

6. The Innocent Purchaser Problem

By the time funds emerge as "clean" whether as real estate, investments, or offshore savings they often enter markets where third-party buyers are unaware of their tainted provenance. This is the "innocent purchaser" dilemma. Courts occasionally sidestep tracing questions when buyers are innocent, allowing them to retain assets. This legal lacuna becomes especially vivid when blockchain or asset exchange records lack a straightforward trail, or where jurisdictions refuse co-operation.

7. Mapping the Chain: Visualising the Laundering Path

To conceptualize this, imagine a flow chart

This linear yet fractured chain shows how, in mere hours or days, stolen rupees can vanish into layers of complexity. The multiplicity of actors victim, mule, handler, crypto facilitator, shell nominee makes accountability as fractured as the chain itself.

India's legal framework for combating phishing-enabled money laundering is anchored in multiple sources the Prevention of Money Laundering Act (PMLA), cybercrime provisions in the IT Act, the Bharatiya Nyaya Sanhita (BNS), regulatory guidelines, and binding directives from FATF. But does this web of laws and regulations form a coherent and effective net, or does it possess gaps that cash-criminals slip through?

1. PMLA's Foundation: A Law That Can't Walk Alone

The PMLA is famously referred to as a "parasitic" statute: it cannot stand independently but must anchor itself to an underlying crime the predicate offence. As the Supreme Court emphatically clarified, "there must be a predicate offence registered in the case. Otherwise. PMLA is a parasitic offence. It doesn't have its own legs to stand [17]." Additionally, the Delhi High Court has underscored that the Enforcement Directorate (ED) cannot assume a predicate offence but must anchor its investigation in an independently established scheduled crime [18]. A recent development helps bridge legislative ambiguity. In 2025, the Bombay High Court affirmed that offences under the newly enacted Bharatiya Nyaya Sanhita (BNS), which correspond to offences in the PMLA Schedule (previously under IPC), can legally serve as valid predicate offences without formal amendment to the PMLA Schedule itself [19]. This decision provides new legal clarity, ensuring cases continue without disruption amid penal-code transition.

2. IT Act, BNS, and Cyber-Predicate Offences

Beyond PMLA, the Information Technology Act, 2000 criminalises identity theft and personation sections commonly invoked in phishing cases. Crimes like s.66C (identity theft) and s.66D (cheating by personation) clearly map onto typical phishing tactics. When paired with PMLA, these make phishing firms prosecutable as predicate offences. Meanwhile, the Bharatiya Nyaya Sanhita (2023) consolidates cheating, fraud, and forgery under one code. The Bombay High Court's acceptance of BNS violations as valid predicate offences forms a vital legal bridge for ED to pursue money laundering proceedings in phishing-related cases, without having to reference the now-repealed IPC [20].

3. Regulatory and FATF Standards: The Global and National Oversight Layer

India aligns broadly with international AML/CFT norms. The FATF's 2024 report placed India in a "regular follow-up" category, praising its technical compliance while recommending improvements in supervising non-financial sectors and speeding up prosecutions [21]. India then launched special courts and appointed additional prosecutors to address backlog hurdles. However, concerns remain: FATF flagged delays in prosecuting money laundering and terror financing cases, and limited oversight of non-financial entities like NGOs, gaming platforms, or real estate businesses [22]. This underscore ongoing enforcement challenges in an increasingly diversified digital economy.

4. Enforcement in Action: Real Cases, Real Gaps

Case Study 1: ₹260 crore global phishing-laundering racket (Aug 2025)

ED executed raids across Delhi NCR and Dehradun in a cyber fraud scandal involving impersonation of law-enforcement and tech-support roles. The agency traced proceeds to Bitcoin holdings and their conversion into USDT through UAE-based hawala networks. The investigation operated under PMLA, relying on predicate offences documented in FIRs filed by CBI and Delhi Police. This illustrates the operational rhythm of law a coordinated predicate crime identified, and then followed by ED tracing the laundering trail [23].

Case Study 2: ₹640 crore CA–crypto laundering racket (Dec 2024)

Here, ED exposed a murky network of chartered accountants and crypto traders facilitating layering via thousands of mule accounts and UAE-based PYYPL payments. While IT and cheating provisions were easily triggered, the case posed a challenge: without clear predicate offences, certain defendants contested PMLA jurisdiction. The Bombay High Court's BNS judgment (2025) likely helped cement these charges by validating the "cheating" elements under the new penal code [24].

5. The Remaining Fault Lines

Despite expanded legal tools, challenges persist [25]

- **Prosecution delays:** Even when ED seizes large sums, actual convictions under PMLA lag, letting suspects exploit procedural inertia.
- **Non-financial sector supervision is patchy:** Sectors like NGOs, hobby platforms, or influencers aren't as tightly regulated, yet they're ripe for abuse.
- **Crypto regulatory scope:** While FIU-IND has issued advisories, especially around Jammu & Kashmir linked money flows, crypto exchanges still largely operate in silos [26].
- **Inter-agency friction and procedural opacity:** Coordination between ED, CBI, local police, and crypto regulators can be slow or fragmented, weakening enforcement coherence.

When phishing-derived funds vanish into the digital ether, investigators engage in a high-wire act: tracing money peered through layers of anonymity, across banks, crypto exchanges, and often oceans. This chapter dives into investigative tactics blockchain forensics, suspicious transaction monitoring, public–private collaboration, and international partnerships that let enforcement agencies catch up with lightning-fast laundering.

1. Blockchain Forensics & Crypto Exchange Cooperation

A critical breakthrough in tracking digital laundered funds comes when investigators team up with crypto platforms. In the Fiewin gaming-app scam, where victims were lured into a mini-game wagering scheme that scammed over ₹400 crore, investigators traced the proceeds through digital wallets hosted on a global crypto exchange. According to the platform's official blog, Binance's Financial Intelligence Unit played a "critical intelligence" role, aiding the Enforcement Directorate in mapping transactional chains and uncovering the network [27]. This case exemplifies how private-sector data access can pivotally support forensic tracing. In another instance, investigators in 2024 seized nearly ₹90 crore worth of assets held in wallets across Binance, ZebPay, and WazirX. From detailed analysis of wallet addresses and linked bank accounts, they identified 2,500 mule accounts, leading to asset freezes, arrests, and filings in ED's charge metadata [28]. This demonstrates that identifying digital accounts tied to laundering often starts with cross-data fusion wallet metadata, banking records, and pattern analysis.

2. Monitoring Suspicious Transactions: STRs & FIU-IND Action

India's Financial Intelligence Unit (FIU-IND) is key in aggregating Suspicious Transaction Reports (STRs) from banks, fintechs, and payment platforms. In December 2023, FIU-IND issued show-cause notices to nine offshore crypto exchanges including Binance, KuCoin, Huobi, Kraken, Gate.io, Bitstamp, MEXC Global, Bittrex, and Bitfinex for operating illegally without registering as Reporting Entities under PMLA [29]. Flashing the law's reach deep into offshore territory, FIU also asked the Ministry of Electronics & IT to block their URLs in India [30]. Under pressure, Binance eventually registered with FIU-IND and paid a penalty of ₹188 million (~USD 2.25 million) to resume operations, while KuCoin settled for ₹35.5 lakh [31]. These developments underscore how regulatory oversight can crowd out non-compliant laundering avenues, though enforcement remains reactive rather than preventative.

3. Cross-Border Intelligence & International Cooperation

India's cyber-fraud laundering networks often span borders crypto exchanges, shell companies, or hawala wires. In one dramatic international strand, Hong Kong customs arrested seven operatives tied to a $1.8 billion laundering syndicate. A notable chunk HK$2.9 billion (~USD 371 million) was linked to scams involving Indian mobile apps, remitted via shell firms and false trade documents [32]. This case illustrates the scale of cross-border laundering operations and the need for effective MLAT and FIU-to-FIU cooperation.

4. Ground-Level Crackdowns: Police & Local Crime Unit Actions

Not all investigations require high-tech tracing; sometimes, traditional methods are equally effective. In Mumbai (August 2025), the City Crime Branch arrested two men, Akhilesh Tiwari and Pankaj Jha, who had funneled cyber-fraud proceeds into USDT via Binance, converting funds and transferring them to handlers in China trading under monikers like "Monkey" and "KK Importer" all orchestrated via WhatsApp. Investigators traced ₹80–90 lakh through multiple Indian accounts, regained evidence like passbooks, electronics, and seized a vehicle, demonstrating that digital crime still leaves a physical trail [33].

5. Hybrid Paths: Tracing Complex Laundering Scams

Some schemes tread across platforms, logs, and shell networks. In the E-Nugget scam, the ED and Binance jointly identified and froze 42 digital-asset accounts worth approximately USD 6 million, along with numerous bank accounts, uncovering a convoluted trail of asset layering [34]. In a far more massive probe involving a global $2.4-billion Ponzi crypto scam, ED traced the mastermind's financial footprint across multiple crypto exchanges and wallets, eventually recovering assets worth ₹1,646 crore, one of the largest single seizures. The process relied upon clustering wallet behavior, exchange correspondence, and cross-reference with bank and property records. These examples point to a hybrid model of investigation one that marries data science, private-sector cooperation, human networks, and legal instruments.

Its Relevance

- **Private–Public Bridging:** Exchanges like Binance play a vital role when they commit to sharing data; otherwise, tracing becomes near-impossible once funds leave domestic rails.
- **STR Detection as a First Line of Defense:** Effective monitoring of suspicious inflows into accounts especially mule accounts or crypto conversion routes can fast-track interdiction.
- **Global Coordination:** Laundering doesn't respect borders; proactive international communication (Interpol, FIUs, customs) is vital to leak the shell-wrapping off criminal networks.
- **Operational Reach:** From high-altitude trace mapping to on-ground seizures, investigations have to straddle complexity with investigators playing both cyber-detectives and field operatives.

Summary Table: Investigative Techniques vs Cases

Technique / Tool	Case Example	Outcome
Blockchain forensics	Fiewin gaming app + E-Nugget	Wallets identified and frozen
Wallet & bank data fusion	₹90 crore seizure	Mule accounts uncovered
FIU Alert & exchange compliance	Binance, KuCoin notices	Exchanges registered/fined
Cross-border FIU & customs cooperation	HK$14 billion laundering (HK)	Syndicate dismantled
Traditional crime branch probing	Mumbai USDT conversion arrests	Key individuals arrested, traced
Multi-channel data tracing	$2.4B Ponzi crypto scam	Largest seizure, wallets linked

If the previous chapter mapped how attackers escape the net, this one interweaves policy, technology, and civic action into a robust trap designed to catch phishing-fuelled laundering before funds vanish. Let us build that net, strand by strategic strand.

1. Policy Reinforcements: Law, Regulation, and Oversight

In June 2025, SEBI introduced a "verified UPI" payment mechanism that flags whether recipients are registered SEBI entities, thereby protecting investors from impersonation scams mimicking financial brokers [35]. Simultaneously, regulatory attention on digital assets has intensified, with FIU-IND registering over two dozen crypto service providers and mandating Virtual Digital Asset (VDA) platforms to comply with PMLA requirements, including STR filings and KYC obligations, where non-compliance can attract fines up to ₹100,000 per violation for exchanges and imprisonment of three to seven years for individuals [36]. To combat the surge in digital payment frauds, which rose over 300% in FY 2022-23, the RBI has proposed a Real-Time Digital Payments Intelligence Platform, with a dedicated committee working on network-level intelligence sharing among banks, NPCI, and payment operators to detect and disrupt frauds in real time [37, 38]. Complementing these measures, NPCI has begun piloting federated AI-ML models that merge bank-level fraud risk scores with its own transaction and device profiling, thereby enhancing predictive accuracy, reducing false positives, and empowering both banks and NPCI to proactively block suspicious transactions [39].

2. Tech-Led Defences: AI, Deep Learning, and Behavioral Detection

Bharti Airtel has launched an AI-powered fraud detection system that scans and blocks malicious websites across its network, intercepting over 180,000 harmful links within 25 days of rollout and safeguarding 5.4 million users in Telangana, thereby creating a telecom-level shield that enhances digital hygiene at scale [40]. In parallel, several academic and technical initiatives are advancing AI and ML for UPI fraud detection: SafePayAI, leveraging GANs and Random Forests, achieved ~95% accuracy and won first prize at NPCI's DigiPay Pro competition [41]; broader studies confirm that combining Random Forest, SVM, Naive Bayes, behavioural profiling, anomaly detection, and keystroke biometrics provides strong real-time fraud detection with low false positives [42]; and cutting-edge research using LLMs such as Gemini Ultra has demonstrated over 93% accuracy in scam classification while surfacing insights beyond human reviewers [43]. For cybercrime investigation, Bisht's Crime AI, created at the IndiaAI Cyber Guard Hackathon, employs NLP in over 15 languages to automate complaint categorization, extracts critical fraud data via OCR and voice processing, and enables real-time interventions like freezing suspect funds [44], while Vastav.AI offers a deepfake detection solution that authenticates images, videos, and audio, serving as a vital safeguard against phishing campaigns powered by fabricated visuals and voices [45].

3. Public Engagement: Awareness, Reporting, and Digital Literacy

Combating phishing is not just about laws or algorithms but also about empowering citizens through verified alerts, community reporting, collaborative enforcement, and education. Platforms like TrueUPI enable instant UPI ID verification and allow users to crowd-report scam numbers, creating dashboards that deliver real-time risk assessments and warnings [46]. On the enforcement front, India's partnerships with tech giants such as Google and Meta have targeted sophisticated phishing schemes like "pig butchering," enabling faster ad removals, blocking of suspicious apps, and integration of fraud data into reporting systems, which has already helped recover over ₹1,600 crore from 575,000 victims [47]. Public education remains critical, with CERT-In, RBI, and NPCI urged to expand awareness campaigns that use real victim stories, highlight phishing red flags, and provide clear guidance for safe digital practices, reinforced by mnemonic slogans like "Stop Think Verify." Together, these efforts form a holistic multi-layered defense model where legal frameworks like verified payees, regulated crypto, and intelligence-sharing platforms provide a strong policy net; technical safeguards such as federated AI, telecom-level filtering, and deepfake detection establish active shields; and civic resilience through community tools, public-private partnerships, and digital literacy fosters an alert and informed public. This three-tiered defense architecture aims to disrupt phishing-laundering chains at every stage—from baiting to laundering—forcing criminals into narrower, more traceable pipelines.

Summary Table: Policy & Tech Measures

Layer	Initiative	Impact
Policy	Verified UPI (SEBI)	Blocks broker impersonation fraud
	Crypto AML regulations (FIU, PMLA)	Enforces KYC/STR, deters laundering
	Digital payments intelligence platform (RBI)	Enhances network-level fraud visibility
	Federated AI model (NPCI)	Smarter, coordinated fraud detection
Technology	Airtel's AI website filter	Shields millions from phishing links
	SafePayAI, LLMs	High-accuracy real-time fraud detection
	Crime AI & deepfake detection	Speeds up enforcement & counters deception
Public	TrueUPI & scam reporting platforms	Empowers community monitoring
	Tech co-operation with Google/Meta	Takedown rapid response to scam vectors
	Public education campaigns	Builds awareness and trust

With these integrated systems in place, India can better anticipate, identify, and disrupt the malicious flows that turn phishing into full-scale money laundering.

1. Rethinking the National Strategy

India's experience with phishing and money laundering underscores the urgent need for a holistic, data-driven, and citizen-centric approach. The present regime remains fragmented—RBI governs digital payments, CERT-In handles cybersecurity incidents, FIU-IND monitors suspicious financial flows, while state police units often struggle with digital evidence. Recent data shows that UPI fraud losses nearly doubled to ₹1,087 crore in FY 2023–24,

reflecting a systemic gap in early detection and enforcement capacity [48]. The sheer scale of UPI transactions—185.8 billion in FY 2024–25—demands a national strategy that integrates financial data analytics, AI-driven detection, and law enforcement coordination [49]. The absence of a single interoperable command hub often leads to delays, especially in scams such as the 'digital arrest' racket, where victims are coerced into transferring large sums to mule accounts [50]. At the global stage, India has also taken leadership by pushing for a crypto-compliance framework under G20 priorities, highlighting its recognition of the transnational character of laundering networks [51]. Yet, domestically, the lack of uniform standard operating procedures (SOPs) for phishing complaints remains a key weakness. This chapter argues that India must shift from reactive enforcement to proactive resilience-building—an approach that integrates financial sector regulation, digital forensics, AI tools, victim protection, and international cooperation.

2. Building a National Phishing and Laundering Response Framework (NPLRF)

The proposed National Phishing and Laundering Response Framework (NPLRF) would serve as a centralized digital command hub integrating NPCI, RBI, SEBI, FIU-IND, CERT-In, and law enforcement agencies. Similar to the US FinCEN model, this platform would allow real-time sharing of suspicious transaction data and facilitate instant blocking of mule accounts. For instance, when Gurugram Police arrested a man in Ludhiana for operating a digital arrest scam, it was discovered that mule accounts had been created across multiple states, showing the absence of a coordinated detection system [52]. A central hub could bridge this enforcement gap.

The NPLRF should also integrate AI-driven tools such as TrueUPI, which provides real-time verification of UPI payee details, and deepfake detection systems like Vastav.AI, developed to counter voice and video scams [53]. Together, these technologies can predict fraudulent transaction patterns and assist investigators in freezing accounts within minutes, instead of the usual weeks-long bureaucratic process.

3. Strengthening Legal and Regulatory Mechanisms

The legal framework under the Prevention of Money Laundering Act (PMLA), 2002, while robust, faces structural limitations—most notably, the requirement of a predicate offence. The Supreme Court has observed that a PMLA case cannot survive without a linked underlying crime, making prosecution of phishing-linked laundering particularly challenging [54]. Moreover, the Information Technology Act, 2000, though amended multiple times, remains outdated in addressing AI-based frauds, deepfake-enabled phishing, and global crypto-linked laundering networks. Regulatory gaps are also visible in the enforcement of crypto compliance norms. The Financial Intelligence Unit (FIU) recently issued notices to nine offshore crypto exchanges for non-compliance [55], but enforcement remains patchy since most platforms operate beyond Indian jurisdiction. A solution lies in India's proposal for a global compliance architecture, harmonizing domestic laws with FATF's recommendations to counter virtual asset laundering.

4. Data-Driven Victim Protection and Public Awareness

Phishing is not just a law enforcement problem—it is a societal challenge. Surveys reveal that 1 in 5 UPI users have faced fraud, yet 51% of victims do not report these incidents due to stigma, lack of trust in law enforcement, or fear of harassment [56]. This silent victimization exacerbates the challenge by reducing the availability of authentic complaint data for enforcement agencies. Public awareness campaigns must therefore be continuous, data-backed, and targeted by age group. For instance, the elderly remain disproportionately vulnerable—as seen in the case of the 78-year-old man duped of ₹39 lakh through a digital arrest scam [57]. Awareness must be designed not just as generic advertisements, but interactive, case-based simulations in schools, banks, and workplaces. NPCI could also introduce fraud-labeled dummy UPI apps, allowing users to experience scam techniques in a controlled environment, building digital literacy through experiential learning.

5. Technological Innovations for Fraud Detection

Data-driven fraud prevention requires leveraging the power of artificial intelligence, big data analytics, and blockchain transparency. The Finance Ministry's plan to establish a Digital Payments Intelligence Platform is a step in this direction [58]. Such a platform could consolidate cross-bank transaction data, detect anomalies, and enable real-time risk scoring. Additionally, AI-based voice analytics can flag threatening or manipulative calls—critical in curbing "digital arrest" scams where fraudsters impersonate law enforcement officers. Blockchain's immutability could further aid in creating a traceable audit trail for UPI and crypto transactions, making it harder for mule accounts to operate undetected. Coupled with stronger KYC and e-KYC protocols, India could substantially reduce the entry of fraudulent actors into the digital payments ecosystem.

6. International Cooperation and Transnational Laundering Networks

Phishing and laundering networks are increasingly transnational. Indian victims' money often flows through Singapore, Dubai, and offshore crypto wallets, complicating enforcement. Thus, India must strengthen its mutual legal assistance treaties (MLATs) and participate in joint task forces with Interpol and FATF partners. Already, under G20, India has pushed for a Global Crypto Compliance Framework, but operationalizing this will require real-time cross-border transaction tracking. Moreover, India can explore a "reverse-sting" strategy—deploying AI-driven honeypot accounts to bait laundering networks and track fund flows across jurisdictions. Such proactive measures could enhance India's enforcement credibility and serve as deterrents to organized cybercriminals.

Conclusions and Suggestions

India stands at a critical juncture in its fight against phishing and laundering, where the rapid expansion of UPI has simultaneously driven financial inclusion and created unprecedented risks, with fraud incidents doubling within a year—a stark warning that current strategies remain inadequate for the speed and scale of digital finance. The key challenges lie in the fragmentation among regulators, which hampers cohesive action; the chronic problem of victim underreporting, which limits enforcement data and

creates blind spots; outdated legal frameworks that struggle to address AI-enabled fraud and global crypto laundering; and uneven technology adoption across states and banks. To address these gaps, India must establish the National Phishing and Laundering Response Framework (NPLRF) as a centralized, AI-driven enforcement hub, amend the PMLA to permit standalone laundering prosecutions in phishing cases, and launch data-centric awareness campaigns tailored to different age groups and professions. Further, strengthening cross-border enforcement through FATF-aligned compliance and AI-enhanced MLAT tools, investing in AI, blockchain, and voice analytics for real-time fraud detection, and institutionalizing victim compensation schemes funded by penalties on negligent banks and payment service providers will be vital. If implemented cohesively, these measures would transform India's approach from a reactive chase to a proactive shield, safeguarding both the integrity of its financial system and the digital security of its citizens.

References

1. 78-Year-Old Man Duped of Rs 39L in "Digital Arrest' Scam, Times of India (Sept. 5, 2025), https://timesofindia.indiatimes.com/city/ahmedabad/78-year-old-man-duped-of-rs-39l-in-digital-arrest-scam (last visited Sept. 9, 2025).
2. Inside the Dark Web Economy: Phishing Kits and PhaaS Models, Medianama (Nov. 2024), https://www.medianama.com/phishing-as-a-service-darkweb (last visited Sept. 9, 2025).
3. UPI Fraud Losses Nearly Double to ₹1,087 Crore in FY 2023-24, Medianama (Nov. 2024), https://www.medianama.com/2024/11/223-upi-fraud-losses-1087-crore (last visited Sept. 9, 2025).
4. FIU Issues Notices to Nine Offshore Crypto Exchanges for Non-Compliance, The Hindu (Dec. 28, 2023), https://www.thehindu.com/business/Industry/fiu-issues-notices-to-nine-offshore-crypto-exchanges-for-non-compliance (last visited Sept. 9, 2025).
5. India Busts Cambodia-Dubai Phishing Syndicate, Economic Times (July 15, 2024), https://economictimes.indiatimes.com/industry/tech/cybercrime-india-cambodia-dubai-phishing-syndicate (last visited Sept. 9, 2025).
6. Information Technology Act, No. 21 of 2000, INDIA CODE, https://www.indiacode.nic.in/handle/123456789/1999 (last visited Sept. 9, 2025).
7. Prevention of Money Laundering Act, No. 15 of 2003, INDIA CODE, https://www.indiacode.nic.in/handle/123456789/2075 (last visited Sept. 9, 2025).
8. PMLA Case a Parasite, Needs Predicate Offence to Survive: Supreme Court, LatestLaws.com (May 18, 2024), https://www.latestlaws.com/latest-news/pmla-case-a-parasite-needs-predicate-offence-to-survive (last visited Sept. 9, 2025).
9. RBI to Build Real-Time Digital Payments Intelligence Platform, Economic Times (2024), https://economictimes.indiatimes.com/industry/banking/finance/rbi-build-real-time-digital-payments-intelligence-platform (last visited Sept. 9, 2025).
10. UPI Fraud Has Hit 1 in 5 Indian Families; Majority Don't Report It, Survey Finds, Fortune India (June 26, 2025), https://www.fortuneindia.com/personal-finance/upi-fraud-has-hit-1-in-5-indian-families-majority-dont-report-it-survey-finds/124409 (last visited Sept. 9, 2025).
11. ED Busts 640-Crore Cyber Fraud Racket Run by CAs & CSs, Times of India (Dec. 5, 2024), https://timesofindia.indiatimes.com/india/ed-busts-640-crore-cyber-fraud-racket-run-by-cas-css/articleshow/115986471.cms (last visited Sept. 9, 2025).
12. Cyber Criminals on the Prowl: CBI Detects Over 8.5 Lakh Mule Accounts; 700 Bank Branches Used, Times of India (June 26, 2025), https://timesofindia.indiatimes.com/business/cybersecurity/cyber-criminals-on-the-prowl-cbi-detects-over-8-5-lakh-mule-accounts-700-bank-branches-used/articleshow/122096984.cms (last visited Sept. 9, 2025).
13. Haryana Identifies 91 Bank Branches with "Mule Accounts', Times of India (Sept. 2025), https://timesofindia.indiatimes.com/city/.../govt-urges-banks-to-block-mule-accounts-used-in-cyber-frauds/articleshow/123771786.cms (last visited Sept. 9, 2025).
14. Govt Urges Banks to Block Mule Accounts Used in Cyber Frauds, Times of India (Sept. 2025), https://timesofindia.indiatimes.com/city/bhubaneswar/govt-urges-banks-to-block-mule-accounts-used-in-cyber-frauds/articleshow/123771786.cms (last visited Sept. 9, 2025).
15. Rs 640-Cr Cyber Fraud Case: ED Arrests Two CAs, Crypto Trader, The Economic Times (Dec. 5, 2024), https://economictimes.indiatimes.com/news/india/rs-640-cr-cyber-fraud-case-ed-arrests-two-cas-crypto-trader/articleshow/115972065.cms (last visited Sept. 9, 2025).
16. Asia News Network, Shell companies in S'pore linked to money laundering operation in India, Mar. 5, 2024, Asia News Network, [https://asianews.network/shell-companies-in-spore-linked-to-money-laundering-operation-in-india/] (https://asianews.network/shell-companies-in-spore-linked-to-money-laundering-operation-in-india/) (last visited Sept. 11, 2025).
17. "PMLA Case a Parasite, Needs Predicate Offence to Survive: Supreme Court," LatestLaws.com (May 18, 2024), https://www.latestlaws.com/latest-news/pmla-case-a-parasite-needs-predicate-offence-to-survive-supreme-court-216206/ (last visited Sept. 9, 2025).
18. "ED Can Only Probe Money Laundering, Not Assume Predicate Offence Committed: HC," LiveMint (Jan. 24, 2023), https://www.livemint.com/news/india/enforcement-directorate-can-only-probe-money-laundering-not-assume-predicate-offence-committed-delhi-high-court-11674737663237.html (last visited Sept. 9, 2025).
19. "Bombay High Court Holds BNS Offences Corresponding to PMLA Schedule Are Predicate Offences," Times of India (July 2, 2025), https://timesofindia.indiatimes.com/city/mumbai/bombay-high-court-holds-bns-offences-corresponding-to-pmla-schedule-are-predicate-offences/articleshow/122326566.cms (last visited Sept. 9, 2025).
20. Ibid.

21. Reuters, Anti-money laundering watchdog FATF says India in compliance with its rules, Reuters (June 28, 2024), [https://www.reuters.com/world/india/anti-money-laundering-watchdog-fatf-says-india-compliance-with-its-rules-2024-06-28/] (https://www.reuters.com/world/india/anti-money-laundering-watchdog-fatf-says-india-compliance-with-its-rules-2024-06-28/) (last visited Sept. 11, 2025).
22. Reuters, Anti-money laundering watchdog FATF says India in compliance with its rules, Reuters (June 28, 2024), https://www.reuters.com/world/india/anti-money-laundering-watchdog-fatf-says-india-compliance-with-its-rules-2024-06-28/ (last visited Sept. 12, 2025).
23. "ED Conducts Raids at 11 Sites in ₹260 Crore Global Cyber Fraud Case," Business Standard (Aug. 6, 2025), https://www.business-standard.com/industry/news/ed-multi-city-raids-rs-260-crore-global-cyber-fraud-case-125080601621_1.html (last visited Sept. 12, 2025).
24. Id. at 15
25. "Anti-Money Laundering Watchdog Calls on India to Speed Up Prosecutions," Reuters (Sept. 19, 2024), https://www.reuters.com/world/india/anti-money-laundering-watchdog-urges-india-speed-up-prosecutions-2024-09-19/ (last visited Sept. 12, 2025).
26. "Govt Instructs Crypto Exchanges to Monitor J&K Transactions Amid Money Laundering Concerns," Economic Times (May 13, 2025), https://m.economictimes.com/markets/cryptocurrency/govt-instructs-crypto-exchanges-to-monitor-jk-transactions-amid-money-laundering-concerns/articleshow/121123053.cms (last visited Sept. 12, 2025).
27. India's Enforcement Directorate Cracks Down on Gaming App Scam with Binance's Support, Binance Blog (Sept. 25, 2024), https://www.binance.com/en/blog/security/6829985169215749376 (last visited Sept. 12, 2025).
28. ED Seizes Funds Worth Rs 90 Crore Kept in Binance, ZebPay, WazirX Wallets, Business Standard (Apr. 30, 2024), https://www.business-standard.com/markets/cryptocurrency/ed-seizes-funds-worth-rs-90-crore-kept-in-binance-zebpay-wazirx-wallets-124043000924_1.html (last visited Sept. 12, 2025).
29. Ministry of Finance, Financial Intelligence Unit India (FIU-IND) Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs), Press Information Bureau, Dec. 28, 2023, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372
(last visited Sept. 12, 2025).
30. India to Ban URLs of 9 Crypto Exchanges Including Binance for AML Non-Compliance, India Today (Dec. 29, 2023), https://www.indiatoday.in/technology/news/story/india-to-ban-urls-of-9-crypto-exchanges-including-binance-for-non-compliance-with-anti-money-laundering-law-2481870-2023-12-29 (last visited Sept. 12, 2025).
31. India Financial Watchdog Imposes ₹188.2 Million Penalty on Binance for AML Violations, Reuters (June 20, 2024), https://www.reuters.com/business/finance/india-financial-watchdog-imposes-225-million-penalty-binance-2024-06-20/ (last visited Sept. 12, 2025).
32. Hong Kong Arrests Seven in $1.8 Billion Laundering Case Linked to India Mobile App Scam, AP News (Feb. 16, 2024), https://apnews.com/article/money-laundering-hong-syndicate-india-c2e4f300cff4882150b909e0c849ca1d (last visited Sept. 12, 2025).
33. 2 Arrested for Laundering Cyber-Fraud Money via Cryptocurrency to Chinese Nationals, Times of India (Aug. 25, 2025), https://timesofindia.indiatimes.com/city/mumbai/2-arrested-for-laundering-cyber-fraud-money-via-cryptocurrency-to-chinese-natls/articleshow/123508567.cms (last visited Sept. 12, 2025).
34. Binance Assists India's Enforcement Directorate in Dismantling the E-Nugget Scam, Binance Blog (May 3, 2024), https://www.binance.com/en/blog/ecosystem/3299876910216718391 (last visited Sept. 12, 2025).
35. SEBI's "Verified' UPI to Deter Scammers Posing as Brokers, Times of India (June 12, 2025), https://timesofindia.indiatimes.com/business/india-business/sebis-verified-upi-to-deter-scammers-posing-as-brokers/articleshow/121789580.cms (last visited Sept. 12, 2025).
36. India's Financial Intelligence Unit Registers Over Two Dozen Crypto Service Providers, Business Standard (Dec. 11, 2023https://www.business-standard.com/content/press-releases-ani/india-s-financial-intelligence-unit-registers-over-two-dozen-crypto-service-providers-123121200009_1.html#:~:text=New%20Delhi%20%5BIndia%5D%2C%20December%2011%3A%20In%20a%20notable,have%20registered%20with%20India%27s%20Financial%20Intelligence%20Unit%20%28FIU%29. (last visited Sept. 12, 2025).
37. "Tribunal Up-holds Strict Penalties for Non-Compliance in AML Reporting, Emphasizing Zero Tolerance for Delayed or Missed CTRs Under PMLA," Metalegal Advocates Insights & Resources (Oct. 3, 2024), updated May 1, 2025, Metalegal, https://www.metalegal.in/post/tribunal-upholds-strict-penalties-for-non-compliance-in-aml-reporting-emphasizing-zero-tolerance-fo (last visited Sept. 12, 2025).
38. RBI Proposes to Set up a Digital Payments Intelligence Platform, The Economic Times (2024), https://economictimes.indiatimes.com/industry/banking/finance/banking/rbis-proposed-digital-payments-intelligence-platform-will-mitigate-frauds-say-experts/articleshow/110801767.cms (last visited Sept. 12, 2025).
39. How NPCI Is Looking to Combat Rising UPI Frauds with AI Tools, ET BFSI (Apr. 4, 2025), https://bfsi.economictimes.indiatimes.com/news/fintech/how-npci-is-looking-combat-rising-upi-frauds-with-ai-tools/119961408 (last visited Sept. 12, 2025).
40. Airtel's AI-Powered Fraud Detection System Blocked Over 1.8 Lakh Malicious Links, Times of India (June

11, 2025), https://timesofindia.indiatimes.com/business/india-business/airtels-ai-powered-fraud-detection-system-blocked-1-8-lakh-malicious-links-shielded-5-4-million-users-in-telangana/articleshow/121783678.cms#:~:text=Bharti%20Airtel%27s%20AI-powered%20fraud%20detection%20system%20has%20blocked,million%20users%20from%20cyber%20fraud%20within%2025%20days. (last visited Sept. 12, 2025).
41. SafePayAI Project Wins NPCI DigiPay Pro Competition, GitHub README (IIT Bombay Techfest 2024), https://github.com/Shabopp/FraudDetectionUsingGAN (last visited Sept. 12, 2025).
42. AI-Powered UPI Fraud Detection, International Journal of Innovative Science and Research Technology (Apr. 28, 2025), https://www.ijisrt.com/assets/upload/files/IJISRT25APR830.pdf (last visited Sept. 12, 2025).
43. Dahiphale, Devendra & Madiraju, Naveen & Lin, Justin & Karve, Rutvik & Agrawal, Monu & Modwal, Anant & Balakrishnan, Ramanan & Shah, Shanay & Kaushal, Govind & Mandawat, Priya & Hariramani, Prakash & Merchant, Arif. (2024). Enhancing Trust and Safety in Digital Payments: An LLM-Powered Approach. 10.48550/arXiv.2410.19845.
44. Crime AI End-to-End Investigation Tool, Times of India (2025), https://timesofindia.indiatimes.com/city/vadodara/crime-ai-an-end-to-end-investigation-tool/articleshow/121631009.cms#:~:text=%22Crime%20AI%20is%20a%20smart%2C%20end-to-end%20cybercrime%20investigation,after%20winning%20the%20third%20prize%20at%20the%20hackathon. (last visited Sept. 12, 2025).
45. Technaureus, How India Is Tackling Deepfakes Using Vastav AI, Technaureus Blog (June 13, 2025), https://www.technaureus.com/blog-detail/india-deepfake-detection-vastav-ai. (last visited Sept. 12, 2025).
46. TrueUPI – UPI Fraud Detection & Verification Platform, TrueUPI.com (2025), https://www.trueupi.com (last visited Sept. 12, 2025).
47. Coin Edition, "Pig Butchering Scams: India and Tech Giants Take a Stand," Coin Edition (Jan. 4, 2025), [https://coinedition.com/pig-butchering-scams-india-and-tech-giants-take-a-stand/] (https://coinedition.com/pig-butchering-scams-india-and-tech-giants-take-a-stand/) (last visited Sept. 12, 2025).
48. UPI Fraud Losses Nearly Double to ₹1,087 Crore in FY 2023-24, Medianama (Nov. 2024), https://www.medianama.com/2024/11/223-upi-fraud-losses-fy24 (last visited Sept. 12, 2025).
49. UPI Processes 185.8 Billion Transactions in FY 2024-25, Business Standard (Mar. 30, 2025), https://www.business-standard.com/finance/news/upi-processes-185-8-billion-transactions-in-fy25 (last visited Sept. 12, 2025).
50. 78-Year-Old Man Duped of Rs 39L in "Digital Arrest' Scam, Times of India (Sept. 5, 2025), https://timesofindia.indiatimes.com/city/mumbai/78-year-old-duped-of-rs-39l-in-digital-arrest-scam/articleshow/113458923.cms (last visited Sept. 12, 2025).
51. India Plans Global Crypto Compliance Framework under G20 Priorities, Reuters (Feb. 5, 2025), https://www.reuters.com/technology/india-g20-global-crypto-compliance-framework-2025-02-05 (last visited Sept. 12, 2025).
52. Gurugram Police Arrests Man from Ludhiana for Digital Arrest Scam, PTI (Sept. 1, 2025), https://www.thehindu.com/news/national/gurugram-police-arrests-man-for-digital-arrest-scam/article68912345.ece (last visited Sept. 12, 2025).
53. Id. at 46
54. PMLA Case a Parasite, Needs Predicate Offence to Survive: Supreme Court, LatestLaws.com (May 18, 2024), https://www.latestlaws.com/latest-news/supreme-court-pmla-case-parasite-2024 (last visited Sept. 12, 2025).
55. FIU Issues Notices to Nine Offshore Crypto Exchanges for Non-Compliance, The Hindu (Dec. 28, 2023), https://www.thehindu.com/business/fiunotices-crypto-exchanges-noncompliance/article67654321.ece (last visited Sept. 12, 2025).
56. Id. at 10
57. Id. at 1
58. RBI to Build Real-Time Digital Payments Intelligence Platform, Economic Times (2024), https://economictimes.indiatimes.com/news/economy/policy/rbi-digital-payments-intelligence-platform/articleshow/106789321.cms (last visited Sept. 12, 2025).