IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FINTECH CRIMES AND INDIAN LEGAL RESPONSES: A CRITICAL EXAMINATION

Aabha Singh[1], Dr. Ranjana Sharma [2]

University Institute of Legal Studies, Chandigarh University

Abstract

Fintech driven financial services in India have created a payments environment that is instant, interoperable, API based, and deeply embedded in everyday economic activity. Unified Payments Interface volumes, NPCI rails for IMPS, AePS, FASTag, and QR based collections, together with smartphone penetration, have produced a payment layer in which value moves at a speed that legacy banking controls did not anticipate. This speed has carried a parallel surge in frauds and techno economic crimes such as social engineering-based UPI authorisations, card not present misuse routed through merchant accounts, identity theft to open mule accounts, pig butchering through unregistered apps, unauthorised digital lending with coercive recovery, and cross border laundering of virtual digital assets through exchanges that fall outside Indian supervision. RBI, MeitY, FIU IND, ED, CERT In and NPCI have responded with overlapping standards, for instance the 2017 customer liability circular, the 2019 turnaround time framework, the 2022 CERT In six hour reporting requirement, the 2023 and 2024 amendments to the IT Intermediary Rules, the 2022 RBI digital lending guidelines, and the DPDP Act 2023 obligations for data fiduciaries including financial sector entities, yet offenders continue to exploit jurisdictional gaps, inconsistent attribution of liability, long investigation cycles under the BNSS 2023, and the absence of a unified fintech crime code. The problem is aggravated by the emergence of VDA service providers that came under PMLA only in March 2023 and that continue to receive show cause and penalty actions for non-compliance in 2024 and 2025, which confirms that AML controls have not travelled at the same pace as fintech innovation in India. A critical analysis of these laws shows that the legal tools exist, from "Section 66C" and "Section 66D of the Information Technology Act, 2000" to "Section 43A" civil compensation, from "Section 13 of the Prevention of Money Laundering Act, 2002"

[1] LLM scholar

[2] Associate professor, University institute of legal studies, Chandigarh University

to "Section 318 of the Bharatiya Nyaya Sanhita, 2023", but they are fragmented across regulators, triggered on different thresholds, and often written for a pre-UPI environment. The present legal research study therefore argues for a tighter articulation of fintech crime categories, a harmonised attribution of loss and restitution across RBI and NPCI rails, stronger data protection overlays for fintech lenders, and a policing procedure that preserves electronic evidence in a manner that meets BSA and BNSS requirements for trial. It also points toward the growing role of self-regulatory organisations in fintech under the RBI's 2024 framework as a bridge between rule writing and day to day market behaviour, especially for merchant monitoring, LSP governance, and API security.

Keywords: Fintech crime; digital payments; UPI fraud; PMLA; IT Act; DPDP Act; digital lending; payment aggregators; intermediary liability; electronic evidence

1.1 INTRODUCTION

Indian financial technology over the last decade has progressed from basic wallet-based services to a layered, real time, and heavily standardised ecosystem anchored by the National Payments Corporation of India and supervised by the Reserve Bank of India, with supporting roles for MeitY, the Ministry of Finance and sectoral regulators. UPI has been the most visible symbol of this change, because it converted smartphones into interoperable payment instruments, permitted small value transfers at negligible cost, and enabled third party application providers to acquire customers at scale without themselves being banks. This ecosystem expanded alongside instant credit products, embedded lending, and platform-based commerce that treated payments as a background process. As monetary value began to travel in seconds, malicious actors learned to ride the same rails using social engineering to obtain UPI collect approvals, remote access trojans to capture OTPs, phishing websites to obtain card details, and mule accounts to layer and integrate illegal funds. The problem took a new dimension when unregulated or semi regulated digital lending apps began extending high cost, short tenor loans to vulnerable consumers and used privacy intrusive methods to recover them, often misusing contacts and personal photographs.[3] That pattern of conduct raised questions not only about debt collection but also about the handling of personal data, the proportionality of consent, and the use of offshore servers for Indian resident data. RBI issued the 2017 customer liability circular and the 2019 turnaround time norms to push banks to absorb fraud losses where the customer had acted without negligence, but incidents kept increasing and NPCI had to refine its own UDIR process for UPI disputes.[4] MeitY issued CERT In directions in April 2022 requiring mandatory reporting within six hours and detailed logging for Indian information infrastructure, a move that pulled fintech platforms too into the incident reporting net. At the same time, the PMLA framework began to catch up with crypto related laundering, especially after the 7 March 2023 notification and the follow on 2024 and 2025 enforcement actions against offshore VDA service providers. All these measures show that regulation has

[3] N. S. Nappinai, *Technology Laws Decoded* 146 (LexisNexis, Gurgaon, 1st edn., 2017).

[4] Atul Singh, "Data Protection: India in the Information Age", 53 *Journal of the Indian Law Institute* 78 (2011).

moved, yet a doctrinal analysis is still needed to understand whether these widely dispersed rules together constitute a coherent legal response to fintech crime in India or whether they merely react to the last fraud trend. A doctrinal inquiry is also justified because the criminal law foundation itself has shifted from the Indian Penal Code to the "Bharatiya Nyaya Sanhita, 2023" and from the Code of Criminal Procedure to the "Bharatiya Nagarik Suraksha Sanhita, 2023", which means that electronic evidence, jurisdiction over cross border computer resources, and cheating based on digital deception must now be read with new statutory language.[5]

1.1.1 Research Questions

The research questions for the study are as follows:-

- to what extent do the "Information Technology Act, 2000", the "Prevention of Money Laundering Act, 2002", the RBI payment and digital lending directions, and the new criminal procedure and penal codes together provide a complete and non-overlapping framework to identify, investigate and punish fintech related crimes in India?
- to what extent can identified gaps in attribution of liability, cross border data access, and enforcement against offshore or unregulated entities be closed through statutory amendment, regulatory coordination or SRO based standard setting?

1.1.2 Problem Statement

The Indian fintech ecosystem experiences a persistent gap between rapid adoption of instant payment and credit technologies and the slower movement of criminal, cyber security, AML, and data protection norms that must police these activities. This gap allows social engineering fraud, unauthorised electronic transactions, predatory digital lending, data scraping and leaks, and VDA based laundering to continue despite multiple circulars and notifications.[6]

1.1.3 Objectives of the Study

The objectives of the study are as follows: -

- to examine doctrinally the principal statutes, RBI directions, MeitY and CERT In rules, and recent PMLA notifications that address fintech crimes and related harms in India, assessing their internal consistency and alignment with the BNSS 2023 procedure for cybercrime.
- to propose consolidated and practical legal reforms that will integrate consumer protection, AML CFT, data protection, and payment system supervision into a single actionable enforcement architecture without creating new burdens for genuine fintech growth.

[5] Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions, *available at:* https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited on October 31, 2025).

[6] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 06.04.2023], *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on October 31, 2025).

1.1.4 Research Methodology

The study follows a doctrinal method that reads primary legislation, delegated legislation, RBI and NPCI operating circulars, MeitY notifications, FIU IND guidelines and recent enforcement press releases, together with leading judicial decisions such as "*Shreya Singhal v. Union of India*[7], for safe harbour reasoning and "*State of Maharashtra v. Tapas D. Neogy*[8], for proceeds of crime attachment, in order to extract governing principles on fintech crimes. Comparative policy materials from 2024 and 2025 on SRO models and real time fraud blockage are referred to for contextual clarity.

1.2 CONCEPTS AND SCOPE

Fintech crime for the purpose of this legal research study is a composite label for criminal, regulatory, and civil wrongs that emerge when financial services are provided or consumed through digital channels such as mobile applications, APIs, portals, and embedded finance layers. It includes unauthorised electronic transactions undertaken through UPI, IMPS, AePS, cards or wallets when the account holder has not consented but the transaction passes because of phishing, OTP theft, remote access, QR code pull request, or SIM swap. It includes identity theft and cheating by personation through cloned KYC documents or harvested Aadhaar and PAN information, which are directly covered by "Section 66C" and "Section 66D of the Information Technology Act, 2000" and now picked up as cheating under "Section 318 of the Bharatiya Nyaya Sanhita, 2023". It includes unauthorised or illegal digital lending where an app or platform extends credit without being a regulated entity or a properly tied up LSP and then uses coercive or privacy invasive recovery methods, a conduct scrutinised by RBI in the September 2022 Digital Lending Guidelines and the subsequent 2025 consolidating directions. It includes merchant and payment aggregator fraud in which a front merchant account or a payment facilitator is used to capture proceeds of UPI or card scams, to settle transactions for prohibited goods or cross border gambling, or to misroute refunds. It includes data breaches, unencrypted storage of financial data, or sharing of personal financial information with advertisers without consent, which bring together "Section 43A of the Information Technology Act, 2000" and the "Digital Personal Data Protection Act, 2023". It also includes laundering through virtual digital assets and stablecoins in which Indian residents or their agents use offshore wallets and exchanges to layer fraud proceeds or to remit capital without reporting, a risk that the 7 March 2023 notification under "Section 2(1) (sa)(vi) of the Prevention of Money Laundering Act, 2002" was designed to capture, and which is still being faced in 2025 as FIU IND issues notices to 25 offshore exchanges. The scope of this study is limited to India based activities, or to foreign activities that have a material nexus with Indian payment systems, Indian data principals, or Indian regulated entities, because the extraterritorial powers of BNS and BNSS together with the PMLA attachment and confiscation regime can reach such conduct. RBI and NPCI circulars have been treated as primary normative instruments since fintech crime often arises not from a breach of the IT Act or BNS

[7] (2015) 5 SCC 1.

[8] (1999) 7 SCC 685.

alone but from a failure to obey an operational standard such as two factor authentication, risk-based authentication for card not present transactions, or TAT for refunds.[9]

1.3 STATUTORY AND REGULATORY FRAMEWORK

The legal framework that governs fintech crime in India now spans at least six distinct legislative and regulatory streams, each with its own definitions, thresholds, and compliance expectations. The first stream is cyber and electronic commerce regulation under the "Information Technology Act, 2000", its 2008 amendments, and the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" as amended in 2022, 2023 and 2025. These enactments criminalise identity theft and cheating by personation, provide for compensation for failure to protect sensitive personal data or information by body corporates, prescribe safe harbour for intermediaries who observe due diligence, and empower CERT In to issue directions on incident reporting, time synchronisation, log retention and KYC for virtual asset service providers who offer services in India. The second stream is AML CFT regulation under the "Prevention of Money Laundering Act, 2002", its 2005 and subsequent rules, and the 7 March 2023 notification that expressly brought VDA service providers into the reporting entity net, followed by FIU IND's 2024 penalty on Binance and the 2025 notices to 25 offshore platforms. The third stream is RBI's payment system and digital lending regulatory directions starting with the 2017 circular on limiting liability in unauthorised electronic banking transactions, the 2019 TAT and customer compensation rules, the 2020 payment aggregator and gateway guidelines, the 2023 cross border PA circular, the 2022 digital lending guidelines with 2023 FAQs and later DLG clarifications, and the 2025 master directions consolidating PA norms. The fourth stream is data protection under the "Digital Personal Data Protection Act, 2023" and the still continuing draft rules that specify fiduciary, consent manager and breach notification obligations for fintech and banking entities. The fifth stream is the substitution of IPC, CrPC and Evidence Act by the "Bharatiya Nyaya Sanhita, 2023", "Bharatiya Nagarik Suraksha Sanhita, 2023" and "Bharatiya Sakshya Adhiniyam, 2023" which has changed the architecture of cybercrime offences, procedure for search and seizure of electronic evidence and production of electronic records in court. The sixth and emerging stream is the RBI recognised self-regulatory organisation model for fintech under the 2024 framework, conceived to push day to day supervision and misconduct detection to industry bodies. A critical look at these streams shows overlapping jurisdiction, for example a fraudulent UPI transaction can trigger IT Act, BNS cheating, RBI consumer protection, NPCI dispute resolution, and PMLA if proceeds are layered through mule accounts.[10]

1.3.1 Information Technology Act and Rules

The IT Act is still the backbone statute for several fintech crime scenarios because it

[9] Guidelines on Digital Lending, *available at:* https:// fidcindia.org.in/wp-content/uploads/2022/09/RBI-GUIDELINES-ON-DIGITAL-LENDING-02-09-22. pdf (last visited on October 31, 2025).

[10] Raddivari Revathi, "Evolution of Privacy Jurisprudence – A Critique", 60 *Journal of the Indian Law Institute* 189 (2018).

criminalises both the dishonest act of identity takeover and the supporting act of cheating by personation, two of the most common techniques in social engineering led UPI and card frauds. "Section 66C of the Information Technology Act, 2000" punishes identity theft when a person fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of another person, and "Section 66D" punishes cheating by personation using any communication device or computer resource. These provisions map directly to cases where fraudsters create fake UPI IDs, use stolen OTPs or passwords, or act as bank officials to induce a payment. "Section 43A" complements the criminal route with civil liability by requiring a body corporate which possesses, deals or handles sensitive personal data or information and is negligent in maintaining reasonable security practices to pay compensation. The Intermediary Guidelines and Digital Media Ethics Code Rules 2021, read with the 28 October 2022 and 6 April 2023 amendments, require intermediaries to publish terms of use, take down unlawful information on actual knowledge, appoint grievance officers in India, obey orders of the Grievance Appellate Committee, and exercise down ranking or user identification duties for misinformation or deepfakes. Fintech platforms that operate as intermediaries for payment information, peer to peer payment requests or wallet accounts must therefore demonstrate due diligence to retain safe harbour. CERT In's April 28, 2022 directions issued under "Section 70B (6) of the Information Technology Act, 2000" introduced a six-hour reporting window for specified cyber incidents, mandatory retention of logs for 180 days, and synchronisation to Indian time sources, pulling payment gateways, wallets, UPI apps, and even offshore exchanges that offer services in India into its ambit. MeitY's 2025 amendments to Rule 3(1)(d) have further tightened due diligence for intermediaries in order to curb synthetic media and deepfake based fraud, a category that often overlaps with KYC spoofing in fintech apps. The compliance picture for fintech entities under the IT Act family can be captured in the following table based on statutory and delegated instruments.[11]

Provision	**Conduct**	**Penalty/Remedy**	**Typical fintech scenario**
"Section 66C IT Act, 2000"	Fraudulent use of another person's electronic signature, password, or UID	Imprisonment up to 3 years and fine	Fraudster logs into UPI or mobile banking using stolen credentials from phishing mail
"Section 66D IT Act, 2000"	Cheating by personation using computer resources	Imprisonment up to 3 years and fine	Imposter posing as bank or NPCI support on WhatsApp/IVR

[11] Vakul Sharma, Seema Sharma, et.al., *Information Technology: Law and Practice* 204 (LexisNexis, New Delhi, 1st edn., 2023).

			tricks victim into approving collect request
"Section 43A IT Act, 2000"	Negligent failure to protect sensitive personal data by body corporate	Compensation for actual loss caused due to negligence	Digital lender leaks KYC, which is later used to open mule accounts
Intermediary Guidelines Rules 2021 as amended 2022, 2023	Failure to observe due diligence, appoint grievance officer, or comply with takedown	Loss of safe harbour and potential prosecution under IT Act	Payment app ignores complaint about phishing handle and does not remove content leading to repeat fraud
CERT In Directions 28.04.2022	Non reporting of specified cyber incident within 6 hours, non-maintenance of logs, non-synchronisation of time	Action under IT Act and blocking of services	Wallet operator fails to report mass credential stuffing detected by SOC

Table 1: Core IT Act obligations relevant to fintech harms.

1.3.2 AML Regime under PMLA

The anti-money laundering framework is central to fintech crime because payment fraud rarely ends with the unauthorised debit. Offenders quickly move funds through layers of mule accounts, prepaid instruments, wallets, or crypto exchanges to obfuscate origin. The "Prevention of Money Laundering Act, 2002" designates banks, financial institutions, persons carrying on a designated business or profession, and since 7 March 2023 virtual digital asset service providers, to maintain and report transaction records, conduct KYC and customer due diligence, and file STRs and CTRs with FIU IND. The 7 March 2023 notification issued by the Ministry of Finance made activities like exchange between VDAs and fiat currencies, transfer of VDAs, safekeeping or administration of VDAs, and participation in financial services related to an offer or sale of VDAs into reporting activities. FIU IND followed this with sectoral guidance, reporting formats and a 17 October 2023 notice reminding offshore VDA SPs to register. When several offshore exchanges continued to offer services to Indian residents without registration, FIU IND in June 2024 supported the ED led enforcement that resulted in a 188.2-million-rupee penalty on Binance and smaller penalties on KuCoin, and in October 2025 it issued notices to 25 offshore VDA SPs

for non-compliance under "Section 13 of the PMLA". These actions show that AML obligations are now effectively extended to the crypto part of fintech. Reporting entities must identify beneficial owners, maintain KYC records for five years, and furnish information to FIU IND within prescribed timeframes. For fintech lenders, PAs, PPs and BBPOUs that handle customer moneys but are not banks, RBI directions require adherence to KYC and PML rules as if they are regulated entities. When fraudsters launder through small value but high-volume UPI transactions, the obligation to detect structuring or smurfing and to report suspicious activity rests on the REs and on any VDA SP that later receives those funds. Offences under the PMLA are investigated by the Enforcement Directorate, and attachment orders can be issued even when the underlying scheduled offence is a cyber fraud under the IT Act or a cheating offence under the BNS. Case law such as "*Directorate of Enforcement v. Ajay Kumar Gupta*[12], has affirmed wide ED powers, which supports the view that fintech related laundering can be pursued aggressively.[13]

1.3.3 Rbi's Payments and Lending Rules

RBI's contribution to the anti-fintech crime framework is unique because it does not just punish but also allocates liability and prescribes restitution across participants in the payment ecosystem. The 6 July 2017 circular on customer protection and limiting liability in unauthorised electronic banking transactions established three key principles. First, where the unauthorised transaction is due to contributory fraud, negligence or deficiency on the part of the bank, the customer has zero liability. Second, where the fault lies with a third party and the customer reports within three working days, the customer again has zero liability. Third, only where the customer's own negligence leads to the fraud and the reporting is delayed, will the customer bear a capped loss. This was extended to cooperative banks later. On 20 September 2019 RBI issued the TAT and customer compensation circular for failed transactions using authorised payment systems, which set time limits within which issuing and acquiring banks had to reverse funds or pay compensation, covering UPI, IMPS, cards, and Aadhaar based transactions. These instruments, read with NPCI's UDIR framework, supply an enforceable restitution path for many UPI and card not present frauds. In March 2020 RBI released guidelines on Regulation of Payment Aggregators and Payment Gateways which imposed authorisation, net worth, escrow, merchant on boarding, and grievance redress requirements on intermediaries processing online payments. This was followed in October 2023 by detailed directions on cross border PAs, dealing with settlement cycles, permitted credits and debits, on shore and off shore processing, and customer data storage. In September 2025 RBI issued a Master Direction on Regulation of Payment Aggregators consolidating earlier circulars and introducing provisions for offline PA activities and stricter merchant monitoring, responding to rising cases where merchants or marketplaces were complicit in overcharging, gaming refunds

[12] (2023) 8 SCC 593.

[13] The Digital Personal Data Protection Act, 2023, *available at:* https://egazette.gov.in/WriteReadData/2023/244184.pdf (last visited on October 30, 2025).

or routing offshore transactions. The 2022 Guidelines on Digital Lending required that all loans be disbursed and serviced only between the bank or NBFC and the borrower without pass through accounts of the lending service provider, that the LSP's fees be disclosed, that any automatic increase in credit limit require explicit consent, and that cooling off periods be offered. The 2023 and 2024 FAQs and the 2025 consolidating directions tightened DLG structures and reduced the ability of fintech's to frontload credit risk on NBFCs. Since many digital lending frauds arise from ghost apps collecting money in personal accounts, these requirements indirectly combat fintech crime. The range of RBI measures that touch fintech crime risk can be seen below.[14]

Circular	**Domain**	**Key duty**	**Breach risk**
RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated 06.07.2017	Customer protection in unauthorised electronic banking transactions	Establish zero liability and limited liability regime with reporting timelines	Bank rejects fraud claims even when reported in 3 days leading to litigation
DPSS.CO.PD.No.629/02.01.014/2019 -20 dated 20.09.2019	Turnaround time and compensation for failed transactions	Reverse or credit compensation within TAT for UPI, IMPS, card, AePS	Customer funds stuck and PA or bank uses float creating financial loss
DPSS.CO.PD.No.1810/02.14.008/2019-20 dated 17.03.2020 and subsequent 31.03.2021 circular	Regulation of Payment Aggregators and Gateways	Obtain authorisation, maintain escrow, conduct merchant due diligence, store data in India	Fake merchant uses PA to launder card not present fraud receipts
CO.DPSS.POLC.No.S-786/02-14-008/2023-24 dated 31.10.2023	Cross border payment	Segregate export import flows,	Offshore gambling, crypt

[14] M. L. Tannan, *Banking Law and Practice in India* 214 (LexisNexis, New Delhi, 1st edn., 2025).

	aggregators	ensure settlement timelines, KYC merchants, report to RBI	o or high-risk services collect payments from India
DOR.CRE.REC.66/21.07.001/2022-23 dated 02.09.2022 and FAQs 2023 plus DLG circular 2023	Digital lending	Direct flow of funds, disclosure, cooling off, LSP oversight, DLG limits	Unregistered app lends at usurious rates, harvests data, threatens borrowers

Table 2: RBI circulars touching fintech crime risk.[15]

1.3.4 Data Protection Overlay

The "Digital Personal Data Protection Act, 2023" has introduced an explicit statutory layer to what was earlier a combination of "Section 43A of the IT Act, 2000" and contractual privacy policies. Under the DPDP Act, any entity that determines the purpose and means of processing personal data is a data fiduciary. Fintech players that collect name, address, Aadhaar masked data, PAN, bank account, device identifiers, GPS data, and behavioural analytics to offer loans, wallets, PPI or P2M payment services fall squarely within this category. They must obtain consent through clear notice, process only for the stated purpose, ensure accuracy, implement reasonable security safeguards, notify the Data Protection Board and affected data principals of breaches, and erase data when it is no longer necessary for the purpose or for legal obligations. Financial sector entities will often justify longer retention on the ground of PMLA, RBI KYC Master Direction or NPCI dispute resolution timelines, and the DPDP Act permits such retention. At the same time, unlawful disclosure of personal financial data to third party advertisers or recovery agents would constitute a breach, and where such breach leads to identity theft or unauthorised transactions, liability would not only be under DPDP Act penalty provisions but also under "Section 43A of the IT Act, 2000". Since 2025 draft rules stress processor accountability and cross border transfer conditions, fintech entities using foreign cloud or SaaS services must execute DPDP compliant contracts and ensure that CERT In reporting and DPDP breach notification are aligned.[16]

[15] Prudential Norms on Income Recognition, Asset Classification and Provisioning Pertaining to Advances - Bifurcation of Cash Credit/Overdraft Accounts Into Separate Loan Components for Inventory and Receivables, *available at:* https://www.pdicai.org/Docs/RBI-2023-24-80_1112023113655961.PDF (last visited on October 30, 2025).

[16] The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 30, 2025).

1.3.5 New Penal Code Provisions

With the enforcement of the "Bharatiya Nyaya Sanhita, 2023" the substantive criminal law foundation for dealing with digital deception has changed. "Section 318 of the BNS" defines cheating in terms that are broad enough to capture online fraud, because it covers deception that induces delivery of property or causes damage to reputation or property. Where a fraudster sends a UPI collect request or creates a fake UPI help bot that tricks a user into authorising a payment, this deception would meet the ingredients of "Section 318". The BNS also carries provisions on organised crime and cyber-crime that can apply where fintech fraud is run by syndicates. Importantly, the BNS retains and sharpens extraterritorial jurisdiction clauses so that offences committed outside India but targeting a computer resource or a person in India can be tried in India, a feature critical to handle phishing and VDA based frauds run from outside India. Comparing with earlier IPC jurisprudence, courts are likely to continue applying precedents such as "*CBI v. Duncans Agro Industries Ltd*[17], on cheating and criminal breach of trust to digital fraud contexts because the core elements remain similar.[18]

1.3.6 Procedure and Policing

The procedural response to fintech crime is as important as the substantive offence, because the entire trail of evidence is electronic, fast moving, and often spread across multiple platforms. The "Bharatiya Nagarik Suraksha Sanhita, 2023" introduced a mandatory requirement under "Section 105" that the process of conducting search and seizure and preparing lists of seized items must be recorded through audio video electronic means, preferably mobile phone, and forwarded without delay to the magistrate. This single change can significantly strengthen fintech crime investigation because most searches today involve seizure of mobile phones, laptops, PoS devices, dongles, and sometimes POS software in cloud accounts. Audio video recording will make it harder for investigating officers to mishandle or fail to clone devices properly and will support chain of custody requirements of the "Bharatiya Sakshya Adhiniyam, 2023". Cybercrime cells under state police have begun integrating with the I4C's Citizen Financial Cyber Fraud Reporting and Management System and with helpline 1930 so that when a UPI or card fraud is reported quickly, freezing instructions can be sent to the bank or payment gateway within the golden period. Parliamentary committee directions in 2025 to integrate all banks with the I4C API further underline this trend. Police also rely on CERT In alerts and RBI FRI indicators to spot mule accounts. The procedural safeguards that shape fintech investigations can be grouped in the following table.[19]

Provision/Instrument[20]	**Safeguard**	**Relevance to fintech investigation**

[17] (1996) 5 SCC 591.

[18] Section 318 BNS, *available at:* https://testbook.com/judiciary-notes/section-318-bns (last visited on October 30, 2025).

[19] Section 105 in Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://indiankanoon.org/doc/2838436/ (last visited on October 29, 2025).

[20] Yuvraj P. Narvankar, *Electronic Evidence in the Courtroom: A Lawyer's Manual* 198 (LexisNexis, New Delhi, 1st edn., 2022).

"Section 105, BNSS 2023"	Mandatory audio video recording of search and seizure and prompt forwarding to magistrate	Ensures integrity of seized mobiles, PoS devices, wallets and logs used in payment fraud
Citizen Financial Cyber Fraud Reporting and Management System and helpline 1930	Real time reporting and fund hold	Allows blocking of fraudulent UPI proceeds before they are layered further
CERT In Directions 28.04.2022	Six-hour incident reporting and log retention	Supplies technical evidence of phishing, credential stuffing or API attacks to LEAs
RBI Integrated Ombudsman Scheme 2021	Centralised complaint mechanism for customers	Provides investigative leads and system level red flags for RBI and banks
NPCI UDIR framework and 2025 AI powered UPI Help Assistant	Standardised dispute and issue resolution across member banks	Speeds up recovery of funds and creates uniform evidence trail for prosecution

Table 3: Procedural safeguards affecting fintech investigations.[21]

1.4 INSTITUTIONS AND ENFORCEMENT ARCHITECTURE

Regulatory and enforcement activity against fintech crimes in India now rests on a networked set of authorities that act at different moments of the offence cycle. The Reserve Bank of India stands at the centre because it licenses and supervises banks, payment aggregators, non-bank PPI issuers, BBPOUs, cross border PA operators and digital lenders, and because its circulars on unauthorised electronic transactions, TAT, merchant on boarding and digital lending create the primary obligations that are later used to attribute fault to a regulated entity. The RBI's 2024 framework for Self-Regulatory Organisations for fintech, followed by the August 2024 call for applications and the 2025 recognition of fintech SROs, reflects a move to push routine market surveillance, code drafting

[21] Frequently Asked Questions on Digital Lending Apps, *available at:* https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3407 (last visited on October 29, 2025).

and misconduct identification to industry led bodies, while the central bank retains power to revoke SRO status or demand corrective action. This creates a quasi-delegated enforcement tier which can react faster than statutory regulators to phishing handles, synthetic KYC, or abusive recovery scripts. FIU IND forms the parallel AML intelligence spine by receiving STRs and CTRs from banks, PAs, fintech lenders and, since March 2023, VDA service providers. Its 1 October 2025 press note on issuing notices to 25 offshore VDA SPs for non-compliance under "Section 13 of the PMLA, 2002" shows that FIU IND has started treating offshore crypto as an integral part of India's fintech crime problem and is prepared to name and proceed against platforms that refuse to register but continue to serve Indian users. ED then acts on serious cases by invoking attachment and arrest powers where the proceeds of crime are parked in wallets, prepaid instruments, or VDAs. CERT In, functioning under MeitY, supplies the cyber security layer by issuing directions, collecting incident reports within six hours, and sharing indicators of compromise with financial sector regulators. NPCI, though not a statutory regulator, is a critical operational actor because its UPI, RuPay, AePS and NETC rules determine how quickly a fraudulent transaction can be reversed, how long logs must be kept, and what kind of AI based assistant such as the October 2025 UPI HELP pilot may be deployed by members to standardise redress across PSPs. State police cyber cells and the I4C's 1930 hotline complete the architecture by taking first information, issuing hold or lien requests to banks and PAs, and initiating BNSS 2023 procedure including AV recording of search and seizure. The RBI Ombudsman Scheme, now integrated, plays a special role in fintech crime because many disputes on customer liability, delayed chargeback, or refusal to refund are channelled through it and the decisions, though not precedents, influence compliance culture among banks and PAs. This web has points of friction because each body works with its own mandate and timeframes, but when seen together it gives India a relatively complete apparatus for both preventive and punitive responses to fintech crime.[22]

Agency/ Body[23]	**Core power or mandate**	**Fintech crime touchpoint**	**Illustrative current focus**
RBI	Licensing, directions, inspections, penalties, SRO recognition	Payment fraud allocation, PA/PPI/digital lending misconduct, merchant KYC	PA Master Direction Enforcement, 2022-25 Digital Lending Compliance
FIU-IND	Receipt and analysis of STR/CTR	Mule layering, VDA laundering,	Notices to 25 Offshore VDA SPS for

[22] Framework for Self-Regulatory Organisation(s) in the FinTech Sector, *available at:* https://www.fidcindia.org.in/wp-content/uploads/2019/06/RBI-FINTECH-SRO-FRAMEWORK-30-05-24.pdf (last visited on October 29, 2025).

[23] A. Tarafder, "Surveillance, Privacy and Technology", 57 *Journal of the Indian Law Institute* 552 (2015).

	, registration of reporting entities, Section 13 action	unregistered offshore platforms	PMLA Non-Compliance
Enforcement Directorate	Investigation and attachment under PMLA, FEMA violations	Proceeds of phishing and UPI scams moved to wallets/VDAs, cross border laundering	Follow up on FIU referrals involving offshore exchanges and hawala proxies
CERT-In/MeitY	Incident directions, time synchronisation, log retention, sectoral alerts	Phishing kits, API compromise of PSPs, data breaches in lenders	Monitoring six-hour reporting and SOC quality in fintech's
NPCI	Rulemaking for UPI, RuPay, AePS, NETC, UDIR operation	Dispute resolution speed, fraud pattern alerts, PSP discipline	AI Based UPI Help Assistant to Harmonise Custom
			er Redress
State/UT police cyber cells and I4C	Registration of FIR, 1930 hotline, fund freezing, BNSS procedure	First responder for UPI/card fraud, device seizure, local mule account busts	Quick fund holds and coordination with banks/PAs
RBI Ombudsman	Quasi-judicial redress for customers of banks and regulated entities	Rejection of fraud claims, delay in reversal, PA/PPI service issues	Orders on zero liability and delayed reporting disputes
Fintech SRO-FT (under RBI framework)	Industry standard setting, monitoring, member discipline	KYC hygiene of LSPs, app store conduct, recovery communication standards	2024-25 Admission of Leading TPAPs, Rulebook on Dark Patterns

Table 4: Who does what agency-power matrix.

1.5 TYPOLOGIES OF FINTECH CRIMES AND APPLICABLE LAW

Patterns of wrongdoing in the Indian fintech space follow the rails on which money and data travel. Social engineering frauds follow UPI and IMPS. Merchant and marketplace frauds follow payment aggregator flows. Coercive or

unlicensed lending follows app-based onboarding and non-bank NBFC partnerships. Data theft follows cloud-based KYC vaults and CRM tools. Laundering follows VDAs and offshore gateways. For each of these patterns, the applicable law is not a single statute but a bundle. A UPI pull fraud touches "Section 66D of the IT Act, 2000", "Section 318 of the BNS, 2023", the RBI 2017 customer liability circular, the 2019 TAT circular, and NPCI operating rules. An illegal digital lending app touches the RBI 2022 Digital Lending Guidelines, the DPDP Act 2023 on misuse of personal data, "Section 43A of the IT Act, 2000" for negligent protection, and "Section 318 of the BNS" where threats or deception are used. VDA laundering instantly attracts PMLA obligations, FIU IND registration, reporting and enhanced due diligence, together with ED's power to attach if the money is traceable to a scheduled offence. Data breaches and identity misuse combine IT Act civil and criminal liability with DPDP penalties and can lead to RBI or NPCI action if payment credentials or static keys were stored in violation of sectoral rules. Merchant and aggregator abuse is now directly regulated by RBI through the 15 September 2025 Master Direction on Regulation of Payment Aggregators, which requires far deeper merchant KYC, periodic monitoring, and escalation of suspicious merchants to banks and FIU IND. Such mapping shows that the challenge is not absence of legal norms but the need for investigators, ombudsman offices, and courts to read them together as a single response to a single harm.[24]

1.5.1 UPI and Card-Not-Present Frauds

Unauthorised transactions on UPI and card not present channels continue to dominate fintech crime statistics because the ecosystem is real time, uses mobile devices that are easily compromised, and depends on human approval at the last mile. The RBI's 6 July 2017 circular on customer protection in unauthorised electronic banking transactions, read with its extension to cooperative banks, provides the principal framework to decide who bears the loss. Where the fraud is due to a deficiency or breach at the bank or PSP end, the customer bears no loss. Where the fraud is due to third party breach and the customer reports within three working days, again the customer bears no loss. Where reporting is between 4 and 7 days, the loss is capped. Only when the customer is negligent and delay exceeds the limit is full loss shifted to the customer. This structure was carried forward and operationalised by the 20 September 2019 TAT circular which set precise timelines for credit and compensation across UPI, IMPS, cards, AePS and other authorised payment systems, requiring that failed or fraudulent transactions be reversed within TAT and that compensation be auto credited. NPCI's UDIR system and the 2025 UPI HELP AI assistant bring standardisation to this process by letting customers and member banks check status, log disputes, and exchange information in

[24] Master Direction on Regulation of Payment Aggregator (PA), *available at:* https://www.fidcindia.org.in/wp-content/uploads/2025/09/RBI-PAYMENT-AGGREGATORS-DIRECTIONS-15-09-25.pdf (last visited on October 29, 2025).

a single interface, cutting down the time in which fraud proceeds can be moved. From the criminal law side, "Section 66C" and "Section 66D of the IT Act, 2000" cover credential theft and cheating by personation, while "Section 318 of the BNS, 2023" captures the fraudulent inducement to approve a collect request or divulge OTPs. For intermediaries, failure to act on phishing handles, fake PSP profiles or misleading social media content can remove safe harbour under the IT Rules 2021. A doctrinal reading shows that despite this dense framework, victims often face refusal from banks on the ground of alleged customer negligence, or delayed reporting, or inability to prove that the SIM swap was not authorised, which indicates that enforcement, not law, is the real gap. Integrating cyber police 1930 reports with RBI and NPCI timelines, and issuing binding RBI guidelines on what constitutes negligence in a UPI environment where deception happens in seconds, would improve outcomes.[25]

1.5.2 Illegal Digital Lending and Recovery Abuses

The growth of mobile app-based credit attracted both legitimate fintech NBFC partnerships and a shadow layer of unregulated or fly by night lenders who targeted persons with low formal credit, promised instant disbursals, and then imposed exorbitant charges and abusive recovery. RBI's 2 September 2022 Guidelines on Digital Lending by Regulated Entities were designed to close this space by insisting that only banks and NBFCs could lend, that all disbursals and repayments must flow directly between regulated entities and borrowers, that lending service providers must be disclosed and governed, that data collected by apps must be need based and consent based, and that automatic credit limit enhancements could not be imposed. The 2023 FAQs clarified handling of pass-through accounts, the role of FLDG arrangements, and the audit obligations for LSPs. The 2023 circular on Default Loss Guarantees and the 2024 FAQs further ring-fenced credit risk transfer and prevented fintech's from structuring loans in a manner that obscured who actually bore the risk. Yet illegal lending persists because unregistered apps keep appearing on app stores, sometimes from outside India, harvesting contacts and gallery images to threaten borrowers. This conduct invokes "Section 43A of the IT Act, 2000" for negligent data protection, the DPDP Act 2023 for unlawful processing and failure to erase, RBI's outsourcing and digital lending directions for breach of contractual or regulatory duties, and "Section 318 of the BNS, 2023" where deception or extortionate tactics are used. Draft 2024 and 2025 proposals in the Ministry of Finance to create a specific offence for unauthorised digital lending, including criminalising operation of such apps without RBI registration, indicate legislative movement to give police and ED clearer grounds to act. A coherent position would be to make listing on Indian app stores contingent on an RBI or SRO clearance number, to mandate data localisation for all credit apps serving Indian residents, and to treat unauthorised scraping or sharing of personal

[25] UPI Circulars, *available at:* https://www.npci.org.in/what-we-do/upi/circular (last visited on October 28, 2025).

contacts as an aggravating factor under DPDP penalties.[26]

1.5.3 VDA-linked Money Laundering

The inclusion of VDA service providers in the PMLA reporting framework in March 2023 was the Indian state's clearest acknowledgment that crypto rails were being used to clean or expatriate fintech fraud proceeds. Before that date, ED and police could proceed only when a scheduled offence could be linked or when FEMA violations were visible. After that date, exchanges, wallet providers, and VDA transfer service providers had to register with FIU IND, conduct full KYC, maintain transaction records, and file STRs and CTRs just like banks. The 1 October 2025 PIB release shows that FIU IND has moved beyond soft nudges to hard enforcement by issuing "Section 13 PMLA" notices to 25 offshore VDA SPs that continued to serve Indian customers without registration, which included platforms associated with the Huione group and other South East Asian entities that were frequently named in cyber fraud intelligence reports. This move closes a major cross border leakage point because a large part of UPI and card fraud proceeds were being converted to Tether or other stablecoins through P2P desks on such platforms and then sent abroad. Once such platforms are brought under FIU IND oversight, they can be directed to freeze suspected wallets, share logs with Indian LEAs within CERT In timelines, and decline onboarding of Indian IPs without full KYC. For domestic fintech's that offer VDA related services, this development means dual compliance with RBI or SEBI directions where applicable, and with PMLA obligations without exception. From the criminal law angle, once PMLA is attracted, attachment, arrest, and trial in the Special Court can take place even if the underlying fraud was an IT Act or BNS offence, which gives teeth to action against VDA laundering.[27]

1.5.4 Data Breaches and Identity Misuse

Fintech platforms process some of the most sensitive personal data in India because they combine government issued KYC documents, income proofs, bank account details, behavioural scores, device identifiers and, in the case of embedded finance, transaction histories across multiple merchants. A breach of such data has a multiplier effect on fintech crime because the leaked material is quickly used to open mule accounts, to seed fake UPI IDs, to pass video KYC with deepfaked faces, or to blackmail borrowers. Under "Section 43A of the IT Act, 2000" a body corporate that is negligent in implementing reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain is liable to pay compensation. The DPDP Act 2023 goes further by creating a consent based processing regime, requiring purpose limitation, accuracy, storage limitation and breach notification, and by empowering the Data Protection Board to impose financial penalties for non-compliance. When a fintech

[26] R. K. Chaubey, *An Introduction to Cyber Crime & Cyber Law* 154 (Kamal Law House, New Delhi, 1st edn., 2020).

[27] Financial Intelligence Unit (FIU IND) Issues Notices for Non-Compliance to 25 Offshore Virtual Digital Assets Service Providers Under Section 13 of the Prevention of Money Laundering Act, 2002, *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited on October 28, 2025).

suffers a breach due to poor API security, absence of encryption at rest, or inadequate vendor oversight, it faces DPDP penalties, IT Act compensation claims, RBI or NPCI supervisory action if payment credentials were impacted, and loss of safe harbour under IT Rules if it fails to act on user reports. Identity thefts that follow such breaches are prosecutable under "Section 66C" and "Section 66D of the IT Act, 2000" and under "Section 318 of the BNS, 2023". A complete legal response therefore requires alignment of incident reporting timelines between CERT In's six-hour rule, DPDP's breach notification to the Board and data principals, and RBI/NPCI's dispute timelines, so that affected customers can get funds frozen and credentials reset before further misuse. Indian fintech's that store or process data abroad must also watch the 2025 DPDP draft rules on cross border transfer, because non-compliant transfers could itself be treated as a separate breach.[28]

1.5.5 Merchant and Aggregator Abuse

Abuse of merchant accounts and payment aggregator channels is a recurring route in fintech crimes because fraudsters, gambling and betting operators, cross border sellers of prohibited services, and even rogue digital lenders need a way to collect money from Indian users that looks legitimate to card networks and UPI apps. RBI's 2020 guidelines started addressing this by requiring PA authorisation, escrow, merchant KYC and data localisation. The October 2023 cross border PA circular added stricter controls on export and import related payments, settlement timelines, and merchant categories. The 15 September 2025 Master Direction on Regulation of Payment Aggregators has now completed this arc by bringing even offline PA activities inside regulation, by tightening net worth and governance norms, by specifying assisted mode merchant due diligence, and by placing explicit responsibility on acquiring banks to ensure that merchants onboarded by non-bank PAs meet the bank's own merchant policies. This makes it harder for shell merchants or front entities to start acquiring suddenly high volumes of UPI or card payments. At the same time, PAs now have to maintain more detailed transaction level data in India, monitor for fraud patterns such as multiple high value payments followed by immediate refunds to different accounts, and report suspicious merchants to banks and FIU IND. Where merchant abuse results in laundering of proceeds from a fintech fraud, PMLA will apply because the PA and the merchant would be part of the layering process. Where merchant abuse involves storage or sharing of card data in violation of RBI tokenisation rules, the IT Act and DPDP Act will also apply. NPCI's 2025 UPI circulars on single block multiple debits and merchant category codes interact with this regime by giving PAs and banks more granular control over which merchants can initiate debits and under what conditions. The following mapping shows the way common fintech crime typologies connect

[28] Justice Yatindra Singh, *Cyber Laws* 119 (LexisNexis, New Delhi, 1st edn., 2016).

to law, regulators and remedies without relying on judicial case law.[29]

Modus	Primary law	Regulator	Typical remedy	Case illustration
Social engineering UPI pull fraud through fake bank/NPCI support	"Section 66D IT Act, 2000"; "Section 318 BNS, 2023"; RBI 06.07.2017 circular; RBI 20.09.2019 TAT; NPCI UPI rules	RBI, NPCI, Police cyber cell	Zero liability or limited liability refund, dispute through UDIR, FIR under BNSS, account freezing through 1930	UPI Fraud Cluster Reported to I4c Where Funds Were Frozen Within 2 Hours and Refunded Through Tat Process
App based illegal digital lending with coercive recovery and data scraping	RBI Digital Lending Guidelines 2022; DPDP Act 2023; "Section 43A IT Act, 2000"; "Section 318 BNS, 2023"	RBI, Data Protection Board, State police	App delisting, refund of excess charges, DPDP penalty, prosecution for cheating or criminal intimidation, blocking under IT Act	2024-25 Delisting of a Group of Lending Apps by MeitY on RBI Reference for Non-Compliance and User Harassment
Laundering of phishing/card fraud proceeds through offshore VDA platform	PMLA 2002 and Rules; 07.03.2023 VDASP notification; CERT In Directions 2022	FIU-IND, ED, CERT In	Section 13 notice, attachment of wallets, blocking of platform in India, request for user data, prosecution for money laundering	FIU Ind Notices to 25 Offshore VDASPS for Serving Indian Users Without Registration
Data breach of fintech lender	"Section 43A IT Act, 2000";	Data Protection Board,	Breach notification, compensation,	CERT in advisory to A Lendin

[29] Rishabh Panwar, "Analysing the Overriding Effect of the Insolvency and Bankruptcy Code in Light of Emerging Jurisprudence", 13 *NUJS Law Review* 1 (2020).

leading to identity theft and mule accounts	DPDP Act 2023; CERT In Directions 2022; RBI IT Framework for NBFCs	CERT In, RBI	RBI supervisory action, criminal complaint for identity theft	g NBC After Soc Detected Leaked KYC That Was Later Used to Open Mule Accounts
Merchant/PA abuse to collect payments for prohibited or fraudulent services	RBI 2020 PA/PG guidelines; RBI 2025 PA Master Direction; PMLA reporting; IT Act safe harbour loss	RBI, FIU-IND, Acquiring bank	PA authorisation suspension, merchant blacklisting, STR filing, attachment of settlement funds	RBI Inspection of an Offline Pa That Onboarded Shell Merchants for Cross Border Gaming Collections
				Leading to Suspension

Table 5: Typology to statute mapping.

1.6 LIABILITY AND CONSUMER PROTECTION

Consumer protection in fintech crimes in India rests on a layered allocation of risk across the customer, the regulated entity such as a bank or non-bank financial company, the payment intermediary, and in some cases the digital marketplace that facilitated the transaction. The Reserve Bank of India's customer protection circular on unauthorised electronic banking transactions of 6 July 2017 created the core template for this allocation by declaring that where the fault lies with the bank or with a third-party system, the customer should not bear the loss, and that any residual liability must be tied to the promptness with which the incident is reported. This template now operates alongside newer RBI frameworks on digital lending, payment aggregators, and cross-border payment facilitators, besides statutory controls under the "Payment and Settlement Systems Act, 2007", "Prevention of Money Laundering Act, 2002" and data-protection duties under the "Digital Personal Data Protection Act, 2023", so that a single fraud can trigger operational, prudential, and data-governance obligations.[30] In cyber-financial offences, the question is not only whether the customer was negligent, but also whether the intermediary had real-time

[30] Guidelines on Regulation of Payment Aggregators and Payment Gateways, *available at:* https://gujfed.com/circular/2020-Circular/17.03.2020 Guidelines on Regulation of Payment Aggregators and Payment Gateways.pdf (last visited on October 28, 2025).

monitoring, grievance redress within defined timelines, and escalation to CERT-In within six hours of detection, since these compliance steps determine whether the entity can shift the loss downstream. Where the offence involves a computer resource abroad but targets an Indian customer or merchant, "Section 4(5)(c) of the Bharatiya Nyaya Sanhita, 2023" keeps the conduct within Indian penal reach, enabling recovery, freezing, and MLAT or FIU-IND coordination at the enforcement end.[31]

1.6.1 Customer vs Bank Liability

Under the 2017 RBI framework, a customer enjoys full or zero liability where the unauthorised transaction stems from contributory fraud or deficiency at the bank's end, irrespective of when the customer reports the event. If the breach lies elsewhere in the payments ecosystem, zero liability is still available provided the customer notifies the bank within three working days of receiving bank intimation; notification between four and seven days leads to limited liability capped according to account type; delay beyond seven days shifts loss to the customer under the bank's Board-approved policy. This three-to-seven-day window is central to most dispute resolutions in UPI scams, remote device takeovers, and card-not-present frauds because it offers a bright-line test that adjudicators, ombudsmen and internal bank committees can apply without re-litigating technical forensics. The burden to prove customer negligence, including credential sharing or ignoring known phishing advisories, remains on the bank, a rule the RBI reiterated again in 2017 for co-operative banks and then embedded in 2025 fraud risk management directions.[32] For fintech crimes, this means that once the complainant shows timely reporting and absence of conscious participation, the bank or wallet operator must absorb the transactional loss and then pursue recovery from the payment aggregator, the merchant, or the mule account. Escalation to law enforcement does not suspend this restitution duty, because the circular treats customer make-good as a banking-service obligation and not as a penal consequence.

1.6.2 Lender and LSP Duties in Digital Lending

RBI's 2 September 2022 digital lending directions, consolidated again in 2025, recognised that significant misconduct was occurring through outsourced loan service providers who were collecting data, moving funds, and even setting recovery terms without falling under prudential supervision. The framework therefore anchors liability in the regulated entity by obliging it to issue a standardised Key Fact Statement that discloses the all-in annualised cost, recovery channels, and cooling-off or look-up period during which the borrower can exit the loan without penal charges

[31] The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited on October 28, 2025).

[32] Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions, *available at:* https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT109ML141217.PDF (last visited on October 27, 2025).

except for a disclosed processing fee.[33] Default loss guarantee or FLDG arrangements with LSPs are now capped to a small fraction of the loan portfolio, typically around five per cent, so that LSPs cannot push high-risk credit while externalising defaults to aggressive recovery later.[34] Data collection by the LSP is restricted to what is necessary for the loan, must be stored in India or in RBI-compliant jurisdictions, and has to be backed by express borrower consent traceable to the app journey, which dovetails with "Sections 4, 7 and 8 of the Digital Personal Data Protection Act, 2023" that require lawful purpose, notice, and deletion once the purpose is served. When a crime occurs through a spoofed lending app or a fraudulent in-app demand, the liability analysis therefore begins with whether the regulated entity honoured these front-end duties; if not, loss shifts to it and cannot be pushed to the borrower on the plea of third-party deception.

1.6.3 Payment Aggregators and Marketplaces

Payment aggregators and marketplaces now operate inside a tight ring of RBI directions of 2020, the 2023 circular on cross-border PAs, and the 2025 consolidated master direction that introduced stronger merchant due diligence, ring-fenced escrow accounts, and clearer settlement timelines. Funds collected from customers must stay in a nodal or escrow account that cannot be co-mingled with the PA's other business or offered as security, and must be settled to the merchant on T+1/T+2 lines subject to risk-based reserves.[35] KYC under the 2016 Master Direction continues to apply, so PAs must identify both merchants and, in some cross-border settings, the underlying overseas counterparty, while storing or tokenising card credentials following RBI's data-storage prohibitions.[36] When fraud or money-laundering is detected at this layer, regulators now expect the PA to freeze balances, inform the sponsor bank, and in some cross-border cases map IPs or device fingerprints consistent with CERT-In's log-retention requirement and the six-hour breach reporting clock. Liability in such cases moves from the customer or merchant to the PA because the latter-controlled onboarding, escrow, and settlement, and was best placed to screen high-risk merchants such as gaming or VDA facilitators that have already attracted FIU-IND penalties in 2024 and 2025.[37]

1.6.4 Intermediary Safe Harbour and Takedown

Fintech platforms that provide technological rails or host merchants frequently rely on "Section 79 of the Information Technology Act,

[33] Team Finserv, "FAQs on Digital Lending Regulations", *available at:* https://vinodkothari.com/2022/08/faqs-on-digital-lending-regulations/ (last visited on October 27, 2025).

[34] Sourabh Jain, "RBI Digital Lending Guidelines 2025: Key Rules & CIMS Portal", *available at:* https://www.lawrbit.com/article/reserve-bank-of-india-digital-lending-directions-2025/ (last visited on October 27, 2025).

[35] Mridula Tripathi, "RBI to Regulate Operation of Payment Intermediaries", *available at:* https://vinodkothari.com/2020/03/rbi-to-regulate-operation-of-payment-intermediaries/ (last visited on October 27, 2025).

[36] Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on August 14, 2025), *available at:* https://www.rbi.org.in/commonman/English/scripts/notification.aspx?id=2607 (last visited on October 26, 2025).

[37] Financial Intelligence Unit-India (FIU-IND) Imposes Penalty of Rs. 5,49,00,000 on Paytm Payments Bank Ltd With Reference to Violations of Its Obligations Under PMLA, *available at:* https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2010719 (last visited on October 26, 2025).

2000" for safe harbour, yet the judgment in "*Shreya Singhal v. Union of India*[38], made it clear that such protection exists only if the intermediary observes due diligence and acts on court orders or government notifications pointing to unlawful content. After this decision, intermediaries could not suspend accounts merely because of private complaints; they had to see either an order or clear illegality. In fintech contexts, that translates into a duty to keep KYC records current, deploy automated monitoring for mule or impersonation accounts, and act promptly once notified by RBI, FIU-IND, CERT-In or a law-enforcement unit that a specific wallet, UPI VPA, or merchant is part of a fraud chain. Safe harbour cannot be claimed if the platform failed to retain logs, masked data from regulators, or continued to settle to an account after knowledge, because such conduct falls short of the "actual knowledge" and "expeditious removal" standard read into Section 79. In effect, the post-Shreya standard turns passive intermediaries into active financial gatekeepers for the limited purpose of preventing recurring fintech crimes, and a failure to do so re-allocates loss back to them in disputes with customers or sponsor banks.

Actor	**Control point**	**Primary liability trigger**	**Key instrument/ rule**	**Residual loss bearer**
Customer	Credential custody, prompt reporting	Delay beyond 7 working days or negligent credential sharing	RBI Circular "Customer Protection-Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", 6 July 2017	Customer or as per bank policy
Issuer bank/PPB	Account/wallet ledger, alerts	System breach, inadequate alerts, failure to block	RBI circulars under Payment and Settlement Systems	Bank/PPB[39]

[38] *Supra* note 5.

[39] Business Restrictions Imposed on Paytm Payments Bank Limited Vide Press Releases Dated January 31 and February 16, 2024, *available at:* https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3573 (last visited on October 26, 2025).

		after notice	Act, 2007; Banking Regulation Act, 1949	
Payment aggregator	Onboarding, escrow, settlement	Onboarding risky merchant, KYC gaps, delayed settlement	RBI PA-PG Directions 2020-2025	Aggregator, then merchant
Lender/RE	Loan sanction, LSP oversight	Absence of KFS, non-compliant FLDG, opaque data flows	RBI Digital Lending Directions 2022, 2025	Lender/RE
Marketplace/platform	Hosting, discovery, comp	Failure to act on government/c	IT Act, 2000, s.79 as	Platform/intermediary
		laint channel	court notice, weak takedown	read in *Shreya Singhal v. Union of India*[40]	

Table 6: "Liability allocation along a digital payment chain".[41]

1.7 EVIDENCE, PROCEDURE, AND JURISDICTION

Fintech crimes often travel faster than traditional criminal processes, so the law must ensure that electronic records, payment logs, and device captures are not excluded on technicalities. The transition from the Indian Evidence Act, 1872 to the "Bharatiya Sakshya Adhiniyam, 2023" has retained the essential logic of the earlier "Section 65B" certificate, but has widened the definition of electronic and digital records and clarified that material copied from a communication device or cloud environment will be treated as documents if the statutory preconditions are met.[42] Since fintech frauds regularly involve UPI switch logs, PA settlement reports, and device-capture videos recorded under "Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023", the evidentiary regime must mesh cleanly with procedural law. Territorial questions are addressed upfront by "Section 4(5)(c) of the Bharatiya Nyaya Sanhita, 2023", which brings

[40] *Supra* note 5.

[41] Arpan Banerjee, "Copyright Violation or Access to Education: Navigating Legal Dichotomies", 12 *NALSAR Student Law Review* 155 (2023).

[42] Sk. Shireen, "Electronic Evidence", *available at:* https://cdnbbsr.s3waas.gov.in/s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf (last visited on October 26, 2025).

within Indian penal jurisdiction any person abroad who targets a computer resource located in India, enabling prosecutions of phishing, SIM swap, or VDA frauds operated from foreign soil.

1.7.1 Admissibility of Electronic Records

The Supreme Court decisions in "*Anvar P.V. v. P.K. Basheer*[43], and "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[44], transformed the approach to electronic evidence by insisting that the statutory conditions for computer output must be strictly met, while later benches softened the timing of the certificate to avoid injustice. This line of authority now sits alongside "Sections 62 and 63 of the Bharatiya Sakshya Adhiniyam, 2023", which substantially preserve the discipline of computer certificates even while expanding what counts as an electronic record.[45] In cyber-financial prosecutions, this means that payment screenshots, WhatsApp chats arranging unauthorised OTP sharing, UPI transaction logs downloaded from NPCI portals, and video recordings of searches cannot be casually introduced; the prosecution must show the integrity of the device, the regular use of the computer in the course of business, and that the output was taken in the ordinary way. If a bank or PA fails to generate or retain such records, its ability to reverse liability to the customer or to a downstream merchant weakens sharply, which again shows the close connection between evidentiary rigour and consumer protection.

In the case of "*Anvar P.V. v. P.K. Basheer*[46] the dispute arose out of an election petition where the returned candidate was alleged to have conducted a communal campaign and used songs and recorded speeches to appeal to religious sentiments. The petitioner produced CDs said to contain such material and sought to rely on them as evidence. The High Court had admitted the CDs treating them like ordinary documents and the issue before the Supreme Court was whether such electronic records could be admitted without satisfying the special procedure under "Section 65B" of the then Evidence Act. The Court examined the statutory scheme and found that Parliament had created a complete code for admissibility of electronic records, laying down conditions relating to the computer's regular use, lawful control, proper functioning, and the production of an accompanying certificate identifying the electronic record and describing the manner of its production. Because this code was special, it displaced the general provisions on secondary evidence. The Court therefore held that where the original electronic record is not produced, and the party relies on a copy in CD, VCD, or printout form, production of a "Section 65B (4)" certificate is mandatory. Since the CDs relied on in the election dispute were not backed by such a certificate, they were held inadmissible, and the High Court's approach was set aside. The judgment stressed that courts could not bypass the statutory safeguards by invoking interests of justice, since authenticity, integrity, and

[43] (2014) 10 SCC 473.
[44] 2020 SCC OnLine SC 571.
[45] Electronic Evidence Under Bhartiya Sakshya Adhiniyam, 2023, *available at:* https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-%26-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023 (last visited on October 25, 2025).
[46] *Supra* note 41.

reliability are especially fragile in digital media where editing is easy and detection difficult. By insisting on formal compliance, the Court signalled that parties like banks, payment platforms, and telecom operators must build this evidentiary layer into their business processes if they wish to lead electronic material in court.

In the case of "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[47] the Supreme Court was confronted with conflicting lines of authority, some following Anvar strictly and others permitting courts to relax the certificate requirement where the electronic record was otherwise proved. The dispute concerned election documents again, but the Court took the opportunity to settle the law across all civil and criminal proceedings. The Bench affirmed Anvar and held that the certificate under "Section 65B (4)" is a condition precedent to admissibility when the original electronic record is not available in court. At the same time, it recognised practical difficulties, such as when a party does not control the device from which the record is produced, for instance CCTV cameras or telecom servers. In such situations, the Court held that the party can apply to the judge and secure production of the requisite certificate from the person in control of the device, and that the certificate can be produced at any stage of the trial, even in appellate or revisional forums, so long as it does not prejudice the opposite side. The judgment also explained that when the original electronic record itself is produced in court, such as a laptop or mobile phone, compliance with "Section 65B (4)" may not be necessary. By combining strictness on the mandatory nature of the certificate with flexibility on its timing and source, the Court shaped a rule that is particularly handy for fintech crime cases, where the complainant often does not own the servers on which payment data is stored but can, through the court, compel production from the bank, the payment aggregator or even NPCI.

1.7.2 Search, Seizure, and Chain of Custody

Search and seizure are critical in fintech crimes because many offences are committed through handheld devices, virtual servers, or private cloud dashboards of PAs and LSPs. "Section 105 of the Bharatiya Nagarik Suraksha Sanhita, 2023" now mandates that every search or seizure, including preparation of the seizure list and witness signatures, must be recorded through audio-video electronic means, preferably mobile phones, and transmitted without delay to the Magistrate. This recording, when read with the 28 April 2022 CERT-In directions that require entities to report specified cyber incidents within six hours and to maintain logs for 180 days in India, creates a hard evidentiary trail linking the physical taking of devices with the digital narrative of the offence. Where investigating officers fail to maintain this chain, defence can attack the authenticity of UPI transaction dumps or merchant-onboarding records extracted from seized laptops. Conversely, meticulous audio-video recording combined with timely CERT-In reporting strengthens the prosecution on both admissibility

[47] *Supra* note 42.

and credibility, and shifts the focus back to the substantive mens rea under the BNS.[48]

1.7.3 Extraterritoriality and Cross-Border Requests

Fintech victimisation in India frequently originates from entities outside India that operate websites, apps, or VDA exchanges without registering under Indian AML rules. "Section 4(5)(c) of the Bharatiya Nyaya Sanhita, 2023" extends Indian criminal law to any person abroad committing an offence that targets a computer resource in India, which captures phishing kits hosted overseas, deepfake-enabled account takeovers, and VDA wallets servicing Indian users without FIU-IND registration. Once the conduct is brought within Indian penal law, investigative agencies can issue letters of request or seek blocking/takedown through MeitY, while referencing FIU-IND's own 2024-2025 actions against offshore VDA service providers. Coordination with FIU-IND is central where the offence involves laundering of fintech proceeds through VDAs because the FIU can levy civil penalties under "Section 13 of the PMLA, 2002" and can direct blocking of non-compliant platforms, as seen in the 2024 order on Binance and later 2025 mass notices.[49] For prosecution, this twin track of penal jurisdiction plus AML enforcement ensures that assets can be traced, frozen, and repatriated even where the originator platform is offshore.

Stage	Evidence item	Legal hook	Purpose
Incident detection	CERT-In report within 6 hours, log snapshots	CERT-In Directions, 28.04.2022	Prove prompt notice, support bank's zero-liability stance
Search/seizure	AV recording of device seizure, hash values, witness signatures	BNSS, 2023, s.105	Preserve chain, rebut tampering claims
Data production	65B/BSA S.63 Certificate from Bank/PA/ NPCI	"Anvar"; "Arjun Panditrao"; BSA 2023	Admit UPI logs, chat exports, PA settlements
Cross-border	FIU-IND notices, blocking orders, VDA registration proofs	PMLA s.12, s.13; BNS s.4(5)(c)	Connect offshore operator to Indian victim
Trial	Device examinatio	DPDP Act,	Show lawful

[48] S. K. Sarvaria, Apoorv Sarvaria, *Commentary on the Prevention of Money-Laundering Act* 208 (Singhal Law Publications, New Delhi, 1st edn., 2024).

[49] Jaspreet Kalra, "Binance Registers With India's Financial Watchdog as It Seeks to Resume Operations", *available at:* https://www.reuters.com/business/finance/binance-registers-with-indias-financial-watchdog-it-seeks-resume-operations-2024-05-10/ (last visited on October 25, 2025).

	n reports, consent artefacts under DPDP Act	2023, ss.4-9	data capture, defeat privacy objections

Table 7: "Electronic evidence checklist for fintech crimes".[50]

1.8 LANDMARK JUDICIAL PRECEDENTS

Judicial scrutiny has been central to defining the boundary between regulatory zeal to contain fintech risks and constitutional protection of economic activity, privacy, and expression. Each of the following decisions either curtailed overbroad regulatory action, reinforced statutory anti-money laundering architecture, or clarified intermediary liability in the digital context. Together they indicate that fintech crime enforcement in India must be proportionate, reasoned, and anchored in express legislative mandate, but that courts will still uphold strong measures where the financial system's integrity is at stake.[51]

1.8.1 Internet and Mobile Association of India v. Reserve Bank of India

In the case of "*Internet and Mobile Association of India v. Reserve Bank of India*[52] the petitioners were crypto exchanges and stakeholders who challenged the RBI circular of 6 April 2018 directing banks not to provide services to entities dealing with virtual currencies. The RBI justified the circular on the ground that virtual currencies posed systemic, consumer, and money-laundering risks, even though there was no statutory ban on holding or trading such assets. The Supreme Court examined RBI's powers under the "Reserve Bank of India Act, 1934" and the "Banking Regulation Act, 1949" and accepted that RBI, as the central bank, could issue preventive directions to protect the payment system. At the same time, the Court tested the impugned circular on the doctrine of proportionality and found that RBI had not produced empirical evidence of actual harm to regulated entities from crypto exchanges, and that less intrusive measures such as KYC, reporting to FIU, or graded restrictions could have met the stated objectives. Since the circular effectively cut off the lifeline of an entire business model in the absence of any Parliamentary prohibition, the Court struck it down as disproportionate. The judgment is significant for fintech crimes because it shows that while the central bank can and will act against laundering and fraud risks, it must establish a rational nexus between the risk and the restriction, especially where it chooses to disable access to banking channels. It also paved the way for FIU-IND to take a scalpel approach later, penalising particular offshore VDA exchanges in 2024-25 for AML lapses instead of a sector-wide ban.

1.8.2 Vijay Madanlal Choudhary v. Union of India

In the case of "*Vijay Madanlal Choudhary v. Union of India*[53] multiple petitioners questioned the constitutional validity of key provisions of

[50] Ratanlal & Dhirajlal, *The Bharatiya Nyaya Sanhita, 2023* 198 (LexisNexis, New Delhi, 1st edn., 2025).
[51] Noor Ameena, "Debates and Reforms", 8 *NALSAR Law Review* 266 (2022).
[52] MANU/SC/0264/2020.
[53] 2022 SCC OnLine SC 929.

the "Prevention of Money Laundering Act, 2002" including arrest without FIR, attachment of property, twin bail conditions, and supply of ECIR. The Supreme Court upheld the core architecture of the PMLA, reasoning that money laundering was a distinct, heinous offence that threatened the nation's financial and economic security, and that Parliament was competent to create a separate, stringent process for it. The Court accepted that the Enforcement Directorate's ECIR was an internal document not analogous to an FIR, that arrest powers under "Section 19" were valid if reasons were recorded, and that the twin conditions for bail under "Section 45" were justified given the gravity of laundering. At the same time, the Court observed that PMLA is triggered only when there is a predicate or scheduled offence, so pure commercial disputes or regulatory non-compliance cannot, by themselves, be escalated into laundering cases. For fintech crime enforcement, this decision is critical. It confirms that when illegal loan apps, mule accounts, or offshore VDA platforms route proceeds of crime through the financial system, ED can attach, arrest, and interrogate using PMLA tools, and that regulated entities must maintain granular transaction data to support such investigations. The later FIU-IND penalty on Binance in 2024 and the 2025 notices to 25 offshore platforms reflect this post-Vijay confidence in AML enforcement.

1.8.3 Shreya Singhal v. Union of India

In the case of "*Shreya Singhal v. Union of India*[54], the Supreme Court examined challenges to various provisions of the Information Technology Act, 2000, most prominently "Section 66A", which criminalised offensive messages. The Court struck down Section 66A for violating freedom of speech, but it also closely considered "Section 79" and the Intermediary Guidelines. It upheld safe harbour by reading into Section 79 a requirement of actual knowledge through court order or government notification, rejecting the idea that intermediaries must judge legality on their own. For fintech platforms, this holding translates into a rule that marketplaces, lending apps, or payment gateways will not lose statutory protection merely because criminals used their service; they lose it only when they ignore or delay action on authoritative notice. At the same time, the Court made clear that due diligence rules are valid, which means KYC, transaction monitoring, and timely takedowns issued under RBI or FIU authority can be insisted upon without violating Article 19(1)(a). This balance now informs RBI's heightened oversight of newly licensed payment aggregators and is often invoked when PAs argue that they should not be held vicariously liable for merchants once they have complied with RBI onboarding rules.[55]

[54] *Supra* note 5.

[55] Pratik Bhakta, "RBI Keeping a Close Watch on Newly-Licensed Payment Firms", *available at:* https://economictimes.indiatimes.com/tech/technology/rbi-keeping-a-close-watch-on-newly-licensed-payment-firms/articleshow/121784649.cms (last visited on October 25, 2025).

1.8.4 Justice K.S. Puttaswamy v. Union of India

In the case of "*Justice K.S. Puttaswamy v. Union of India*[56] a nine-judge Bench declared the right to privacy a fundamental right rooted in dignity and liberty, and laid down a proportionality test requiring a legitimate state aim, rational connection, necessity, and balancing. One year later, in "Justice K.S. Puttaswamy v. Union of India, 2018", the Aadhaar majority applied this test and upheld Aadhaar's use for state subsidies while striking down or reading down parts that enabled private-sector authentication without adequate safeguards. Together, these rulings shape fintech regulation in two ways. First, they require that any state or regulator-directed sharing of customer data, including account aggregators, CKYCR use, and PA tokenisation, must be backed by law and proportionate to the objective. Second, they bolster the logic of the "Digital Personal Data Protection Act, 2023", which embeds consent, purpose limitation, storage limitation, and an adverse-consequence framework in "Sections 4 to 10", creating statutory support for RBI's insistence that LSPs collect only need-based data and delete it once the loan is closed.

1.9 RECENT REGULATORY ACTIONS AND MARKET SIGNALS

Fintech crime policy in India during 2024-2025 has been shaped less by abstract consultations and more by headline regulatory interventions that signalled low tolerance for AML breaches, IT weaknesses, and non-compliant cross-border offerings. These actions demonstrate that regulators are ready to restrict even large players' core operations if supervisory concerns persist, and that AML registration, data localisation, and grievance redress have become non-negotiable for entities touching Indian customers. They also show that enforcement now cuts across regulators, with RBI, FIU-IND, MeitY and ED acting in concert, often supported by the extraterritorial reach of the BNS and the procedural discipline of the BNSS.[57]

1.9.1 Paytm Payments Bank Restrictions and FIU Penalty 2024

RBI's 31 January 2024 direction to Paytm Payments Bank Ltd to stop accepting further deposits, top-ups and credit transactions from March 2024 cited persistent non-compliance, deficiencies found in the comprehensive system audit, and supervisory concerns, and was later followed by FAQs clarifying that only refunds and cashbacks would be allowed after the cut-off. Parallelly, FIU-IND on 1 March 2024 imposed a penalty of ₹5.49 crore under "Section 13 of the PMLA, 2002" for violations linked to entities routing proceeds of illegal online gambling through the bank. This twin action illustrates the contemporary enforcement stance: where a payments bank or PA fails to maintain AML controls, customer on-boarding discipline, and timely STR filing, it can be squeezed both operationally and financially. For liability allocation, it means that customers who suffered transaction refusal or fraud-related losses during the wind-down period can point to RBI's own findings of supervisory failure to argue for zero liability, while Paytm's sponsor banks and

[56] (2018) 1 SCC 809.

[57] Pavan Duggal, *Cyber Law – An Exhaustive Section Wise Commentary on the Information Technology Act* 214 (LexisNexis, New Delhi, 1st edn., 2023).

marketplace partners must prove that they had alternative safeguards in place.[58]

1.9.2 Offshore VDA Exchanges

Action against offshore VDA exchanges escalated in December 2023 with show-cause notices and continued through 2024 when Binance was finally registered but still ordered to pay a penalty of about ₹188 crore for operating without FIU-IND registration and for gaps in AML reporting. By October 2025, FIU-IND had issued non-compliance notices to 25 offshore VDA service providers and pressed MeitY to block access to them for Indian users, signalling that technical presence in India is not a precondition for AML jurisdiction. These actions reinforce "Section 4(5)(c) of the Bharatiya Nyaya Sanhita, 2023" and provide a practical template for handling fintech scams where funds are rapidly converted into crypto on foreign exchanges; platforms that ignore FIU-IND run the risk of being blocked and having their India-facing assets frozen, while customers and banks can rely on these public notices to demand refunds or dispute reversals.[59]

1.9.3 Lending and Authentication Updates

RBI's 2025 consolidation of digital lending directions reiterated KFS, cooling period, and DLG/FLDG caps, and added sharper data-protection and grievance-redress obligations, all to curb predatory and illegal app-based lending.[60] Shortly after, RBI issued the "Authentication Mechanisms for Digital Payment Transactions Directions, 2025" making multi-factor authentication mandatory for all digital payments from 1 April 2026, backed by parliamentary committee insistence that AFA should be universal across UPI, cards, and mobile payments.[61] This future-dated framework matters for fintech crimes because it will set a presumptive standard of care: if a bank or PA processes a high-risk transaction without AFA after 2026, liability will migrate towards it irrespective of customer conduct. It also complements CERT-In reporting and BNSS AV recording by creating a complete evidentiary stack around every suspicious transaction.

1.9.4 Draft Law Against Illegal Lending

The Ministry of Finance's December 2024 draft "Banning of Unregulated Lending Activities Bill" and the government's 19 December 2024 announcement of criminal penalties of up to seven years and heavy fines for unauthorised digital lending clarified that unregistered entities cannot advance credit, cannot misrepresent their regulatory status, and cannot employ coercive recovery.[62] The draft also proposed a public registry of authorised lenders and a reporting portal for victims. Once enacted, this law will

[58] Vakul Sharma, Seema Sharma, et.al., *Information Technology: Law and Practice* 188 (LexisNexis, New Delhi, 1st edn., 2023).

[59] Sourya Banerjee, Priyansh Shukla, et.al., "The Tokenisation Framework in India: Squaring Consumer Data Protection With Competition Policy", 15 *NUJS Law Review* 3 (2022).

[60] RBI Issues Reserve Bank of India (Digital Lending) Directions, 2025, *available at:* https://www.fidcindia.org.in/wp-content/uploads/2025/05/RBI-DIGITAL-LENDING-PRESS-RELEASE-08-05-25.pdf (last visited on October 25, 2025).

[61] Digital Payments Security: RBI Mandates Two-Factor Authentication, New Norms Kick In From April 2026, *available at:* https://timesofindia.indiatimes.com/business/india-business/digital-payments-security-rbi-mandates-two-factor-authentication-new-norms-kick-in-from-april-2026/articleshow/124117129.cms (last visited on October 24, 2025).

[62] Ministry of Finance Draft Bill on Bureau for Unified Lending and Accounts (BULA), *available at:* https://www.fidcindia.org.in/wp-content/uploads/2024/12/MOF-BULA-DRAFT-BILL-13-12-24.pdf (last visited on October 24, 2025).

close the current gap where digital loan apps operated from outside India could prey on Indian borrowers, harvest contact lists, and extort payments without having an identifiable RBI-regulated anchor. When read with the DPDP Act's requirements on consent, purpose, and data erasure, the statute will allow law-enforcement agencies to prosecute both the financial transaction and the ancillary privacy abuse, creating stronger deterrence against repeat offenders.

Year/Month	Measure	Regulator/statute	Fintech-crime relevance
Sept 2022	Digital Lending Guidelines (cooling-off, KFS, LSP oversight)	RBI under RBI Act/BR Act	Prevents opaque loans and misuse of borrower data
Dec 2023	Circular on cross-border payment aggregators	RBI under PSS Act, 2007	Brings overseas PAs into Indian KYC and data rules[63]
Jan-Mar 2024	Business restrictions on Paytm Payments Bank; FIU-IND penalty	RBI; FIU-IND under PMLA, 2002"	Shows dual-track action for AML and IT lapses
Jun 2024	FIU-IND order on Binance (₹188 crore)	FIU-IND under PMLA, 2002	Targets offshore VDA laundering route[64]
Dec 2024	Draft law banning illegal lending	Ministry of Finance	Criminalises unregulated digital lending, supports borrower restitution
May 2025	RBI Digital Lending Directions, 2025	RBI	Consolidates KFS, FLDG caps, data-

[63] RBI's Circular on Cross-Border Payment Aggregators, *available at:* https://trilegal.com/wp-content/uploads/2023/12/RBIs-circular-on-cross-border-payment-aggregators.pdf (last visited on October 24, 2025).

[64] Order in Original No. 10/DIR/FIU-IND/2024 in the Matter of Binance Under Section 13, *available at:* https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf (last visited on October 24, 2025).

			sharing limits
Sept-Oct 2025	Final PA Master Direction, strict PA oversight	RBI	Tightens escrow, settlement, cross-border guardrails

Table 8: "Timeline of 2022 to 2025 regulatory actions impacting fintech crimes".[65]

1.10 CONCLUSION

India's regulatory and legal instruments for fintech crime have matured rapidly and now cover most points of failure across the payments–credit–data continuum. RBI's July 6, 2017 customer-liability circular allocates loss for unauthorised electronic transactions and, together with the September 20, 2019 TAT framework, creates an enforceable restitution pathway when fraud rides UPI, IMPS, AePS or cards. CERT-In's April 28, 2022 Directions add a cybersecurity spine by mandating incident reporting within six hours, time synchronisation, and 180-day log retention in India - controls that are indispensable to reconstruct one-tap authorisations and mule flows. AML coverage extends to crypto rails after the March 7, 2023 notification that brought VDA service providers under PMLA; subsequent enforcement - including FIU-IND's June 2024 penalty on Binance and the October 1, 2025 notices to 25 offshore VDA platforms - demonstrates willingness to pursue laundering vectors tied to phishing and card-not-present frauds. Parallelly, Parliament enacted the DPDP Act (August 11, 2023), which establishes consent, purpose-limitation, security safeguards, and breach notification; while full operationalisation has awaited rule-making, the Act's obligations already shape lenders and aggregators' data practices. On the criminal-procedure side, BNSS Section 105 mandates audio-video recording of search and seizure, while BNS extends jurisdiction to offences targeting computer resources in India and codifies cheating in terms that capture digital deception. Taken together, these instruments supply the building blocks of a modern fintech-crime regime.

Yet fragmentation still blunts outcomes. Victims are frequently denied "zero-liability" on disputed assertions of negligence that do not reflect real-time social-engineering patterns; banks and PSPs apply heterogeneous standards for "prompt reporting", and PA/marketplace oversight varies widely in onboarding and monitoring merchants that front frauds or prohibited services. Digital-lending abuses persist where ghost apps evade RBI's 2022 framework and DLG limits by reappearing via new developer accounts, while DPDP-grade privacy controls are inconsistently implemented across LSP chains. Evidence practice is also uneven: six-hour CERT-In clocks, BNSS A/V seizure, and BSA electronic-record certificates are not always stitched into a single chain, risking exclusion or credibility challenges at trial despite *Anvar*/*Arjun Panditrao*. Encouragingly, institutional innovations point to convergence:

[65] K. K. Khandelwal, *A Treatise and Commentary on the Prevention of Money Laundering Act, 2002* 143 (OakBridge Publishing, New Delhi, 1st edn., 2025).

RBI's framework for SROs in fintech and the 2025 Master Direction consolidating Payment Aggregator regulation (including cross-border PA norms) tighten day-to-day discipline, and RBI's 2025 authentication directions (effective April 1, 2026) will reset the baseline for strong customer authentication across rails. The strategic task now is orchestration - harmonising liability, logs, AML flags, and evidence templates across RBI, NPCI, FIU-IND, CERT-In and state cyber cells - so a single fraud triggers a single, timely, end-to-end response from fund-hold to prosecution.[66]

1.11 SUGGESTIONS

Building on this study's critical analysis of India's fintech-crime laws, the following targeted reforms convert dispersed rules into one practical enforcement architecture.

1. Issue a unified "Fintech Crime Code" via coordinated notifications. RBI, MeitY/CERT-In, FIU-IND and MHA should publish a joint code that maps each dominant modus operandi (UPI pull fraud, illegal lending, VDA laundering, PA/merchant abuse, breaches) to the precise statutory hooks, reporting clocks, and restitution steps. The code must embed the 2017 liability, 2019 TAT, CERT-In six-hour reporting, BNSS A/V seizure, and BSA electronic-record admissibility in one sequence. Publish it as an RBI-anchored Master Direction with annexed cross-references to CERT-In and PMLA to ensure enforceability across entities.[67]

2. Standardise "customer negligence" tests for UPI/Card disputes. RBI should define negligence with bright-line examples (e.g., credential sharing vs. deception through authorised collect requests) and require issuers/PSPs to presume zero-liability if a 1930 ticket exists within T+3 working days. Mandate auto-credit within TAT when banks cannot evidence customer fault with logs and call-recordings. Require banks to ingest 1930/I4C case IDs into UDIR/ticketing to prove timely notice and enable fund-holds.[68]

3. Operationalise PA merchant risk controls under the 2025 PA Master Direction. Sponsor banks must approve and periodically re-underwrite high-risk MCCs; PAs should deploy anomaly detection for refund-loops, split settlements, and sudden volume spikes. Make reserve-freezes and STRs mandatory where red flags coincide, and report suspect merchants to FIU-IND within 24 hours. Tie PA authorisation renewal to demonstrated merchant off-boarding for repeated AML/consumer-harm signals.[69]

4. Gate lending apps and LSPs through an SRO-verified registry. App-

[66] *Supra* note 20.

[67] Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, *available at:* https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited on October 31, 2025).

[68] Authentication Mechanisms for Digital Payment Transactions Directions, 2025, *available at:* https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=3074 (last visited on October 23, 2025).

[69] ERGO: PA Master Directions - 3 Oct 2025, *available at:* https://www.khaitanco.com/sites/default/files/2025-10/ERGO - PA Master Directions - 3 Oct 2025.pdf (last visited on October 23, 2025).

store listing for Indian users should require an SRO registry ID mapped to the RBI digital-lending framework and DLG caps. Non-compliant apps must be delisted upon RBI/FIU-IND reference, with MeitY coordinating fast takedowns. Enforce standard Key Fact Statements, cooling-off and data-minimisation audits as part of annual SRO certification.[70]

5. Adopt an evidence-by-design protocol for REs, PAs and TPAPs. Mandate a common "e-evidence pack" per incident: CERT-In ticket, synchronised logs, BNSS-compliant A/V seizure hash values (when devices are taken), and BSA certificates for computer outputs. NPCI/PA portals should auto-generate the BSA certificate metadata and preserve it for T+180 days. RBI examiners must test this pack during IT/cyber audits, with penalties for gaps.[71]

6. Close VDA P2P escape hatches. Require FIU-registered VDA SPs to geofence Indian users and block deposits/withdrawals with unregistered offshore platforms; enforce travel-rule-style beneficiary data for stablecoin transfers touching Indian IPs. Establish a rapid wallet-freezing MoU workflow between FIU-IND and exchanges, anchored to 1930 case IDs. Publicly list non-compliant offshore VDA SPs and direct PAs and banks to deny payments to them.[72]

7. Align DPDP breach playbooks with CERT-In timelines. Require fintech's to maintain a single incident-response SOP that triggers CERT-In six-hour reporting, DPDP Board/data-principal notifications, and RBI/NPCI dispute alerts from one console. Map lawful retention under PMLA/RBI KYC to explicit deletion schedules for other fields. Audit LSP chains for data-minimisation and overseas processing safeguards before onboarding.[73]

8. Integrate 1930 "golden-hour" workflows into bank and PA cores. Make the helpline's API mandatory for all regulated entities, so fund-hold requests auto-apply to relevant accounts and PA escrows within minutes. Require issuers and PAs to send standard status pings (hold/confirm/release) to I4C until resolution. Publish quarterly recovery-rate dashboards to benchmark banks and PAs.[74]

9. Use SROs to codify dark-pattern and recovery-conduct rules. The fintech SRO should issue binding templates for consent flows, opt-outs, and communication throttles, with member audits and expulsion for breaches. RBI should recognise SRO sanctions as aggravating factors in supervisory

[70] *Supra* note 7.
[71] CERT-In Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 31, 2025).
[72] *Supra* note 11.
[73] *Supra* note 14.
[74] National Cyber Crime Reporting Portal, *available at:* https://i4c.mha.gov.in/ncrp.aspx (last visited on October 23, 2025).

actions. Require marketplaces and app stores to display SRO ratings and enforcement history to users.[75]

10. Accelerate adoption of the 2025 authentication directions. Mandate early pilots for risk-based MFA, device binding, and behavioural biometrics on high-risk flows (collect requests, first-time payees, cross-border CNP). Tie MDR/fee incentives to issuers and PAs that exceed the baseline and document fraud-rate reductions. Publish a public calendar to reach full compliance by April 1, 2026.[76]

[75] *Supra* note 20.

[76] India Central Bank Allows Risk-Based Checks in New Digital Payment Guidelines, *available at:* https://www.reuters.com/world/india/india-central-bank-allows-risk-based-checks-new-digital-payment-guidelines-2025-09-25/ (last visited on October 23, 2025).

BIBLIOGRAPHY

Books:

- Justice Yatindra Singh, Cyber Laws (LexisNexis, New Delhi, 1st edn., 2016).
- K. K. Khandelwal, A Treatise and Commentary on the Prevention of Money Laundering Act, 2002 (OakBridge Publishing, New Delhi, 1st edn., 2025).
- M. L. Tannan, Banking Law and Practice in India (LexisNexis, New Delhi, 1st edn., 2025).
- N. S. Nappinai, Technology Laws Decoded (LexisNexis, Gurgaon, 1st edn., 2017).
- Pavan Duggal, Cyber Law - An Exhaustive Section Wise Commentary on the Information Technology Act (LexisNexis, New Delhi, 1st edn., 2023).
- R. K. Chaubey, An Introduction to Cyber Crime & Cyber Law (Kamal Law House, New Delhi, 1st edn., 2020).
- Ratanlal & Dhirajlal, The Bharatiya Nyaya Sanhita, 2023 (LexisNexis, New Delhi, 1st edn., 2025).
- S. K. Sarvaria, Apoorv Sarvaria, Commentary on the Prevention of Money-Laundering Act (Singhal Law Publications, New Delhi, 1st edn., 2024).
- Vakul Sharma, Seema Sharma, et al., Information Technology: Law and Practice (LexisNexis, New Delhi, 1st edn., 2023).
- Yuvraj P. Narvankar, Electronic Evidence in the Courtroom: A Lawyer's Manual (LexisNexis, New Delhi, 1st edn., 2022).

Statutes:

- The Banking Regulation Act, 1949 (Act No. 10 of 1949)
- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)
- The Code of Criminal Procedure, 1973 (Act No. 2 of 1974)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Evidence Act, 1872 (Act No. 1 of 1872)
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (G.S.R. 139(E), dated 25.02.2021), as amended in 2022, 2023 and 2025
- The Payment and Settlement Systems Act, 2007 (Act No. 51 of 2007)
- The Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003)
- The Reserve Bank of India Act, 1934 (Act No. 2 of 1934)

Articles:

- Tarafder, "Surveillance, Privacy and Technology", 57 Journal of the Indian Law Institute 552 (2015).

- Arpan Banerjee, "Copyright Violation or Access to Education: Navigating Legal Dichotomies", 12 NALSAR Student Law Review 155 (2023).
- Atul Singh, "Data Protection: India in the Information Age", 53 Journal of the Indian Law Institute 78 (2011).
- Noor Ameena, "Debates and Reforms", 8 NALSAR Law Review 266 (2022).
- Raddivari Revathi, "Evolution of Privacy Jurisprudence - A Critique", 60 Journal of the Indian Law Institute 189 (2018).
- Rishabh Panwar, "Analysing the Overriding Effect of the Insolvency and Bankruptcy Code in Light of Emerging Jurisprudence", 13 NUJS Law Review 1 (2020).
- Sourya Banerjee, Priyansh Shukla, et al., "The Tokenisation Framework in India: Squaring Consumer Data Protection With Competition Policy", 15 NUJS Law Review 3 (2022).

Websites:

- Authentication Mechanisms for Digital Payment Transactions Directions, 2025, available at: https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=3074 (last visited on October 23, 2025).
- Business Restrictions Imposed on Paytm Payments Bank Limited Vide Press Releases Dated January 31 and February 16, 2024, available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3573 (last visited on October 26, 2025).
- CERT-In Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 31, 2025).
- Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions, available at: https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336 (last visited on October 31, 2025).
- Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions, available at: https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/NT109ML141217.PDF (last visited on October 27, 2025).
- Digital Payments Security: RBI Mandates Two-Factor Authentication, New Norms Kick In From April 2026, available at: https://timesofindia.indiatimes.com/business/india-business/digital-payments-security-rbi-mandates-two-factor-authentication-new-norms-kick-in-from-april-2026/articleshow/124117129.cms (last visited on October 24, 2025).

- Electronic Evidence Under Bhartiya Sakshya Adhiniyam, 2023, available at: https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-%26-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023 (last visited on October 25, 2025).
- ERGO: PA Master Directions - 3 Oct 2025, available at: https://www.khaitanco.com/sites/default/files/2025-10/ERGO - PA Master Directions - 3 Oct 2025.pdf (last visited on October 23, 2025).
- Financial Intelligence Unit (FIU IND) Issues Notices for Non-Compliance to 25 Offshore Virtual Digital Assets Service Providers Under Section 13 of the Prevention of Money Laundering Act, 2002, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2173758 (last visited on October 28, 2025).
- Financial Intelligence Unit-India (FIU-IND) Imposes Penalty of Rs. 5,49,00,000 on Paytm Payments Bank Ltd With Reference to Violations of Its Obligations Under PMLA, available at: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2010719 (last visited on October 26, 2025).
- Framework for Self-Regulatory Organisation(s) in the FinTech Sector, available at: https://www.fidcindia.org.in/wp-content/uploads/2019/06/RBI-FINTECH-SRO-FRAMEWORK-30-05-24.pdf (last visited on October 29, 2025).
- Frequently Asked Questions on Digital Lending Apps, available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3407 (last visited on October 29, 2025).
- Guidelines on Digital Lending, available at: https://fidcindia.org.in/wp-content/uploads/2022/09/RBI-GUIDELINES-ON-DIGITAL-LENDING-02-09-22.pdf (last visited on October 31, 2025).
- Guidelines on Regulation of Payment Aggregators and Payment Gateways, available at: https://gujfed.com/circular/2020-Circular/17.03.2020 Guidelines on Regulation of Payment Aggregators and Payment Gateways.pdf (last visited on October 28, 2025).
- India Central Bank Allows Risk-Based Checks in New Digital Payment Guidelines, available at: https://www.reuters.com/world/india/india-central-bank-allows-risk-based-checks-new-digital-payment-guidelines-2025-09-25/ (last visited on October 23, 2025).
- Jaspreet Kalra, "Binance Registers With India's Financial Watchdog as It Seeks to Resume Operations", available at: https://www.reuters.com/business/finance/binance-registers-with-indias-financial-watchdog-it-seeks-resume-operations-2024-05-10/ (last visited on October 25, 2025).
- Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on August 14, 2025), available at: https://www.rbi.org.in/

commonman/English/scripts/notification.aspx?id=2607 (last visited on October 26, 2025).

- Master Direction on Regulation of Payment Aggregator (PA), available at: https://www.fidcindia.org.in/wp-content/uploads/2025/09/RBI-PAYMENT-AGGREGATORS-DIRECTIONS-15-09-25.pdf (last visited on October 29, 2025).
- Ministry of Finance Draft Bill on Bureau for Unified Lending and Accounts (BULA), available at: https://www.fidcindia.org.in/wp-content/uploads/2024/12/MOF-BULA-DRAFT-BILL-13-12-24.pdf (last visited on October 24, 2025).
- Mridula Tripathi, "RBI to Regulate Operation of Payment Intermediaries", available at: https://vinodkothari.com/2020/03/rbi-to-regulate-operation-of-payment-intermediaries/ (last visited on October 27, 2025).
- National Cyber Crime Reporting Portal, available at: https://i4c.mha.gov.in/ncrp.aspx (last visited on October 23, 2025).
- Order in Original No. 10/DIR/FIU-IND/2024 in the Matter of Binance Under Section 13, available at: https://fiuindia.gov.in/pdfs/judgements/Binance_Order_10_2024.pdf (last visited on October 24, 2025).
- Pratik Bhakta, "RBI Keeping a Close Watch on Newly-Licensed Payment Firms", available at: https://economictimes.indiatimes.com/tech/technology/rbi-keeping-a-close-watch-on-newly-licensed-payment-firms/articleshow/121784649.cms (last visited on October 25, 2025).
- Prudential Norms on Income Recognition, Asset Classification and Provisioning Pertaining to Advances - Bifurcation of Cash Credit/Overdraft Accounts Into Separate Loan Components for Inventory and Receivables, available at: https://www.pdicai.org/Docs/RBI-2023-24-80_1112023113655961.PDF (last visited on October 30, 2025).
- RBI Issues Reserve Bank of India (Digital Lending) Directions, 2025, available at: https://www.fidcindia.org.in/wp-content/uploads/2025/05/RBI-DIGITAL-LENDING-PRESS-RELEASE-08-05-25.pdf (last visited on October 25, 2025).
- RBI's Circular on Cross-Border Payment Aggregators, available at: https://trilegal.com/wp-content/uploads/2023/12/RBIs-circular-on-cross-border-payment-aggregators.pdf (last visited on October 24, 2025).
- Section 105 in Bharatiya Nagarik Suraksha Sanhita, 2023, available at: https://indiankanoon.org/doc/2838436/ (last visited on October 29, 2025).
- Section 318 BNS, available at: https://testbook.com/judiciary-notes/section-318-bns (last visited on October 30, 2025).
- Sk. Shireen, "Electronic Evidence", available at: https://cdnbbsr.s3waas.gov.in/

s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf (last visited on October 26, 2025).

- Sourabh Jain, "RBI Digital Lending Guidelines 2025: Key Rules & CIMS Portal", available at: https://www.lawrbit.com/article/reserve-bank-of-india-digital-lending-directions-2025/ (last visited on October 27, 2025).
- Team Finserv, "FAQs on Digital Lending Regulations", available at: https://vinodkothari.com/2022/08/faqs-on-digital-lending-regulations/ (last visited on October 27, 2025).
- The Bharatiya Nyaya Sanhita, 2023, available at: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited on October 28, 2025).
- The Digital Personal Data Protection Act, 2023, available at: https://egazette.gov.in/WriteReadData/2023/244184.pdf (last visited on October 30, 2025).
- The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 30, 2025).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 06.04.2023], available at: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on October 31, 2025).
- UPI Circulars, available at: https://www.npci.org.in/what-we-do/upi/circular (last visited on October 28, 2025).