IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Legal And Regulatory Challenges In Digital Banking In India

Akansha [1] , Dr. Gaurav Khanna [2]

University Institute of Legal Studies, Chandigarh University

Abstract

Digital banking in India has moved from a peripheral channel of service delivery to the centre of banking operations, driven by the Reserve Bank of India's layered regulatory model, the public digital infrastructure created around UPI, Aadhaar and consent-based data sharing, and the growing expectations of customers for frictionless, remote and real-time financial services. At the core of this expansion lies a complex regulatory architecture anchored in the "Reserve Bank of India Act, 1934", the "Banking Regulation Act, 1949", the "Payment and Settlement Systems Act, 2007" and a wide array of master directions, guidelines and FAQs issued by the RBI's supervisory departments, especially for digital lending, payment aggregation, IT outsourcing and KYC. These regulatory instruments, read together with the "Digital Personal Data Protection Act, 2023" that classifies banks as data fiduciaries and with the CERT-In Directions of 28 April 2022 that compel six-hour reporting of cyber incidents, generate a web of concurrent, often overlapping obligations for banks, NBFCs and their fintech partners. Digital onboarding remains a critical risk zone because lenders depend on non-face-to-face identification, assisted V-CIP, Aadhaar-based e-KYC through regulated KUA/Sub-KUA arrangements, and large-scale outsourcing of KYC processing, which heightens exposure to fraud, data breach and impersonation. The RBI's Digital Lending Guidelines of 2 September 2022, the subsequent DLG/FLDG circular of 8 June 2023 and the 2025 tightening on provisioning for fintech-backed guarantees have tried to ring fence balance sheet lending and make credit intermediation traceable, yet frictions persist in loan disbursement flows, in disclosure of annualised cost to borrowers, in segregation of LSP accounts, and in recovery practices that operate on digital channels. Cybersecurity and data governance have acquired sharper contours because the DPDP Act requires purpose

[1] LLM scholar

[2] Associate Professor, University Institute of Legal Studies, Chandigarh University.

limitation, consent logs and breach notification to the Data Protection Board, while CERT-In insists on domestic log storage and rapid incident reporting, and the RBI's 2023 IT Outsourcing Directions insist that supervisory access must survive even multi layered subcontracting. Customer protection sits in the middle of these regimes because customers transact on UPI, cards, wallets and aggregator led checkouts without always dealing directly with a bank, so allocation of liability for failed, delayed or fraudulent transactions must be inferred from RBI's PA directions, NPCI rule books and the BNS/BSA provisions on electronic records and fraud. The enforcement trajectory from 2022 to 2025 shows the RBI becoming more intrusive, extending PA supervision to offline transactions, tightening merchant due diligence, imposing capital and fit-and-proper criteria on non-bank intermediaries, and repeatedly reminding regulated entities that outsourcing of KYC, IT or collections does not outsource responsibility. The reform roadmap therefore lies in clearer statutory anchoring of RBI's digital directions under the PSS Act, harmonising DPDP consent artefacts with the mature AA framework, creating interoperable reporting rails between RBI and CERT-In, and writing sectoral rules that allow proportionate KYC for low value accounts while preserving audit assured traceability for higher risk products.

Keywords: Digital banking; Reserve Bank of India; Payment and Settlement Systems Act, 2007; Digital Personal Data Protection Act, 2023; CERT-In Directions (2022); KYC Master Direction (updated 2025); Digital Lending Guidelines (2022)

1.1 INTRODUCTION

Digital banking in India emerged out of a distinctive convergence of public policy on financial inclusion, affordable telecommunications, interoperable payments and a proactive central bank that interpreted its statutory mandate to include granular operational guidance for all regulated entities. From 2016 onwards, Aadhaar enabled e-KYC, Jan Dhan accounts, and the explosive growth of UPI created an environment in which remote account opening, low value digital payments and platform-based credit delivery could reach millions of users at costs that traditional branch led banking could not match. At the same time, the RBI continued to rely on the "RBI Act, 1934" and the "Banking Regulation Act, 1949" to issue directions to banks and NBFCs in public interest, to call for information, to conduct offsite surveillance and to impose penalties, which meant that every layer of digital delivery was still expected to meet prudential, AML and consumer-protection standards that had been designed for a world of physical branches and paper records.[3] The arrival of the "Payment and Settlement Systems Act, 2007" allowed the RBI's DPSS to authorise payment system operators, prescribe standards, and issue data localisation, tokenisation and merchant onboarding rules, but digital banking soon went beyond pure payments and entered domains such as embedded credit, BNPL, cross border collections and aggregator

[3] Nandan Nilekani, Viral Shah, *Rebooting India: Realizing a Billion Aspirations* 176 (Penguin Books, New Delhi, 1st edn., 2015).

led marketplaces, where the legal status of participants was not always clear. Parallel to this, India legislated for digital privacy and cybersecurity through the Information Technology Act, 2000 and sectoral CERT-In directions; by 2023-24 this framework was replaced or overlaid by the "Digital Personal Data Protection Act, 2023" which treated banks, NBFCs, payment aggregators and even consent managers as data fiduciaries who must record consent, issue notices and report breaches to the Board, irrespective of whether a particular processing operation was also subject to RBI inspection.[4] This created what may be called regulatory layering in digital banking, because the same dataset or transaction could be simultaneously governed by RBI's KYC Master Direction, by a PSS Act authorisation condition, by DPDP obligations, by CERT-In's six hour reporting rule and by NPCI's operating circulars. Banks and their partners needed to design systems that satisfied all of these regimes even when timelines, definitions and thresholds did not align. Outsourcing and cloud adoption increased the problem, since the RBI's "Outsourcing of Information Technology Services Directions, 2023" and its later guidance on operational resilience insisted that business continuity, data access and audit rights must remain with the regulated entity, even if the service was delivered by a large technology provider or a fintech platform.[5] The growth of digital banking undoubtedly advanced financial inclusion because customers in tier 2 to tier 6 centres could open accounts, receive remittances, pay school and utility bills, or seek small ticket credit without visiting a branch, but it also generated systemic risks that arise from technology concentration in a few cloud or API service providers, from deeply nested outsourcing chains, and from the operational centrality of NPCI and other quasi regulatory bodies that sit outside the RBI Act yet control essential rails. The challenge for legal analysis is to examine whether the present framework, built out of circulars and master directions, is adequate for this new scale or whether Parliament, the RBI and allied regulators should articulate a clearer, more harmonised digital banking code.[6]

1.1.1 Research Questions

The research questions for the study are as follows:-

1. To assess whether the existing RBI, PSS Act and DPDP instruments together provide a complete and coherent regulatory framework for end-to-end digital banking, including payments, digital lending, remote onboarding, data sharing and cyber incident handling in India, without creating unmanageable overlaps or gaps for regulated entities and their outsourced partners?
2. To evaluate the extent to which current rules on KYC, FLDG, payment aggregation, account aggregation and

[4] 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).

[5] Master Direction On Outsourcing Of Information Technology Services, *available at:* https://fidcindia.org.in/wp-content/uploads/2023/04/RBI-OUTSOURCING-OF-IT-SERVICES-10-04-23.pdf (last visited on October 25, 2025).

[6] Shehnaz Ahmed, "Rise of Decentralised Finance | Reimagining Financial Regulation", 18 *Indian Journal of Law and Technology* 12 (2022).

cyber reporting actually mitigate the risks of fraud, misuse of Aadhaar, data leakage and loss of customer confidence, and to identify legal and procedural reforms that would align BNSS/BSA evidence and investigation requirements with real time, API driven financial services?

1.1.2 Problem Statement

Digital banking entities operating in India confront concurrent compliance obligations from the RBI's master directions, from the DPDP Act, from CERT-In's 28 April 2022 Directions and FAQs, and from NPCI's product specific rule books, with each instrument prescribing different definitions, reporting formats, retention periods and supervisory touchpoints, which creates fragmentation of accountability, higher operational costs, and legal uncertainty for banks, NBFCs, payment aggregators, fintech lending service providers and consent intermediaries when they collaborate to deliver fully digital products.[7]

1.1.3 Objectives of the Study

The objectives of the study are as follows:-

1. To map the regulatory perimeter of digital banking in India as it currently emerges from the RBI Act, the BR Act, the PSS Act, DPDP Act 2023, CERT-In Directions and the criminal procedure framework under the BNSS, and to correlate this perimeter with the actual business models employed by banks, NBFCs, payment aggregators, account aggregators and fintech LSPs.
2. To analyse the principal friction points in digital lending, KYC and Aadhaar use, data governance, cybersecurity and consumer redress, to study recent enforcement actions and clarificatory circulars, and to advance a set of legal and supervisory measures that promote clarity, proportionality and technological neutrality.

1.1.4 Research Methodology

The study proceeds on the doctrinal method and examines primary sources such as the "RBI Master Direction-Know Your Customer (KYC) Direction, 2016" as updated till 14 August 2025, the "Guidelines on Digital Lending dated 2 September 2022", the "Outsourcing of Information Technology Services Directions, 2023", the "Master Direction on Regulation of Payment Aggregators, 2025", the "Digital Personal Data Protection Act, 2023", CERT-In's Directions issued under "Section 70B of the Information Technology Act, 2000" and key judgments of the Supreme Court including "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[8], and "*Vijay Madanlal Choudhary v. Union of India*[9], (2022) 10 SCC 1", together with authoritative commentaries and government FAQs to derive the legal position.[10]

[7] 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).

[8] (2017) 10 SCC 1.

[9] 2022 SCC OnLine SC 929.

[10] 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).

1.2 LEGAL AND INSTITUTIONAL ARCHITECTURE

The legal and institutional architecture of digital banking in India is characterised by the primacy of the RBI as the banking and payments regulator, assisted by the National Payments Corporation of India as the standard setting and operating body for UPI, RuPay and several retail rails, and supplemented by sector agnostic regulators such as the Data Protection Board under the DPDP Act and CERT-In under the Information Technology Act. The RBI draws its principal powers from the "Reserve Bank of India Act, 1934" and the "Banking Regulation Act, 1949", under which it may issue directions in public interest, call for information, inspect books, and impose monetary penalties or supervisory restrictions such as business caps, onboarding freezes and IT rectification plans. These powers have been used extensively from 2020 onwards to regulate even those activities, like digital lending through LSPs or payment aggregation by non-bank entities, that are not expressly spelled out in the parent statutes but are considered integral to the stability and integrity of the financial system. The PSS Act created a parallel gatekeeping regime, so that any person wanting to operate a payment system, including a PA, PPI issuer or card network, must obtain authorisation and adhere to standards set by the DPSS. The institutional picture is further complicated by quasi regulatory instruments issued by NPCI, which is a not-for-profit company but whose circulars are treated by member banks as binding because participation in UPI and related systems is critical to business. CERT-In, established under "Section 70B of the Information Technology Act, 2000", cuts across sectors and enforces cybersecurity hygiene, log retention and breach reporting, while the DPDP Act introduces for the first time a statutory consent manager that can overlap with the RBI's own Account Aggregator architecture. This ecosystem operates without a single unifying legislation on digital banking, which means harmonisation must be achieved through coordinated circulars, through industry level standardisation and, in the longer term, by suitable amendments to the PSS Act and allied laws.[11]

1.2.1 Rbi's Powers and Instruments

The RBI's authority to steer digital banking primarily flows from "Section 35A of the Banking Regulation Act, 1949" which empowers it to issue directions to banking companies in public interest, in the interest of banking policy, or to prevent the affairs of any banking company being conducted in a manner detrimental to the interests of the depositors. This provision, read with "Sections 21 and 35 of the BR Act" and "Sections 45JA, 45L and 45M of the RBI Act, 1934", was expressly invoked in the RBI's 2 September 2022 Digital Lending Guidelines to bring lending service providers and digital lending apps inside the supervisory vision of the RBI even though many of them were not themselves banks or NBFCs. By using this power, the RBI required that all loan disbursements and repayments in digital lending transactions must flow directly between the bank or NBFC account and the borrower account, with no pass through or pooling in the accounts of LSPs, that fees payable to LSPs must be paid by the regulated

[11] N S Nappinai, *Technology Laws Decoded* 212 (LexisNexis, Gurgaon, 1st edn., 2017).

entity and not charged to the borrower, that a Key Fact Statement must be delivered digitally, and that complaints relating to digital lending apps must be dealt with under the RBI's consumer grievance redress framework.[12] Similar reliance on "Section 35A" and kindred provisions can be seen in the "Outsourcing of IT Services Directions, 2023" where the RBI insisted that outsourcing cannot dilute the regulated entity's compliance obligations, that RBI must have unconditional access to data, and that arrangements involving cloud, API gateways or fintech platforms must have termination and audit clauses broad enough to meet supervisory expectations. Because these instruments are issued under statutory authority, non-compliance by a bank, NBFC, PPI issuer or PA can trigger penalties, restrictions on partner onboarding, or even directions to discontinue an outsourced or partnership-based product, which in digital banking can temporarily incapacitate a large customer base.

1.2.2 Payment and Settlement Systems Act

The "Payment and Settlement Systems Act, 2007" constitutes the second pillar of digital banking regulation because it empowers the RBI to regulate and supervise all payment systems, to issue policy directions, to determine standards, to call for returns, and to authorise or refuse authorisation to non-bank entities who wish to operate as system providers. Under "Section 18 of the PSS Act" the RBI issued the 2020 guidelines on regulation of payment aggregators and payment gateways and, after consultations and interim amendments, replaced them with the comprehensive "Master Direction on Regulation of Payment Aggregators, 2025" which now covers domestic online PAs, physical PAs, cross border PAs and merchant acquiring standards.[13] These directions impose minimum net worth requirements, prescribe escrow arrangements with scheduled commercial banks, prohibit PAs from storing card credentials beyond tokenisation allowances, lay down timelines for settlement to merchants, and, in the 2025 iteration, extend obligations to vet merchants, monitor their transaction level activities and prevent the use of PA rails for prohibited or unverified goods and services. Because most digital banking products route their collections, refunds or recurring mandates through payment systems, the PSS Act regime effectively sets the operational ground rules for digital banking even when the underlying product is a loan or a deposit. The PSS Act also provides the legal basis for tokenisation, card on file restrictions and data localisation for payment data, which are enforced through DPSS circulars and directions, and which in practice require banks and PAs to architect data storage in India and to contractually bind their overseas vendors to Indian rules.

1.2.3 Data Protection and Privacy

With the coming into force of the "Digital Personal Data Protection Act, 2023" all banks, NBFCs, PAs, AAs and even fintech LSPs who determine the purpose and mean of processing personal data are treated as data fiduciaries and must comply with obligations relating to consent,

[12] Digital Lending Guidelines, *available at:* https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3413 (last visited on October 23, 2025).

[13] 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).

notice, data minimisation, purpose limitation, data security, data principal rights and breach notification. This is a significant shift from the earlier position where banks primarily relied on "Section 43A of the IT Act, 2000" and the 2011 SPDI Rules and took the view that compliance with RBI's outsourcing, KYC and electronic banking security guidelines was adequate. Under the DPDP Act, consent must be free, specific, informed, unconditional and unambiguous, and banks must be able to prove that such consent was obtained, which dovetails with but is not identical to the consent artefacts used in the RBI's Account Aggregator framework. The Act expressly contemplates the role of consent managers who will manage, review or withdraw consent on behalf of data principals, a role that maps naturally onto NBFC-AAs, and several commentaries in 2025 have argued that operating AAs should be deemed consent managers under the DPDP Act to avoid duplication and disruption.[14] For digital banking this means that every onboarding journey, whether through mobile app, assisted BC, V-CIP or AA based data pull, must embed DPDP compliant notices and controls and must be capable of logging withdrawals of consent and acting on them in reasonable time. Breach notification to the Data Protection Board and to affected data principals is mandatory, and penalties for non-compliance can go up to ₹250 crore, adding a fresh enforcement vector distinct from RBIs. This privacy regime must also be harmonised with "Sections 61, 63, 64 and 65 of the Bharatiya Sakshya Adhiniyam, 2023" which govern the admissibility and integrity of electronic records, since banks must collect, preserve and produce electronic evidence of customer consent, KYC documents, V-CIP recordings and transaction logs for investigative or judicial proceedings.[15]

1.2.4 Cyber Incident Reporting

Cyber incident reporting in India is governed by the CERT-In Directions dated 28 April 2022 issued under "Section 70B(6) of the Information Technology Act, 2000" which require all service providers, intermediaries, data centres, body corporates and government organisations to report specified cybersecurity incidents to CERT-In within six hours of noticing such incidents or being brought to notice. This requirement applies squarely to banks, NBFCs, payment aggregators and their managed service providers, and because the Directions also require retention of ICT system logs for 180 days in India, synchronisation of time servers, and furnishing of information sought by CERT-In, digital banking arrangements must ensure that their outsourced or cloud-based infrastructure can meet these mandates. Since 2023, RBI's own alerts and the 2024-25 operational resilience guidance have highlighted that reporting to CERT-In does not absolve regulated entities from reporting to RBI, and that supervisors may call for root cause analysis, patching and customer communication within tight timelines.[16] For incidents involving

[14] Reconciling The Account Aggregator And Consent Manager Frameworks, *available at:* https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/ (last visited on October 31, 2025).

[15] The Bharatiya Sakshya Adhiniyam, 2023 (No. 47 Of 2023), *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 30, 2025).

[16] India Cenbank Issues Guidance Note On Operational Risk Management And Resilience, *available at:* https://www.reuters.com/world/india/india-cenbank-issues-guidance-note-operational-risk-management-resilience-2024-04-30/ (last visited on October 29, 2025).

customers and payment systems, NPCI also expects incident reports, which can lead to three parallel reporting lines. This multiplicity necessitates internal playbooks in banks and PAs that can categorise incidents, collect forensically sound evidence as required by the BSA, and file within six hours while still maintaining accuracy.[17]

Source/Instrument[18]	**Core obligation**	**Coverage across bank-fintech chain**
RBI Directions under "Section 35A of the BR Act, 1949" and relevant Master Directions (Digital Lending 2022, IT Outsourcing 2023, KYC 2016 updated 2025)	Maintain end-to-end accountability for customer funds, data and KYC, ensure disbursement and repayments go directly between RE and customer, board approved IT outsourcing and grievance redress, V-CIP equivalence, business continuity, RBI access to logs	Applies to banks, NBFCs, HFCs, PPI issuers, PAs wherever reference is made to Regulated Entities and to all third-party service providers through contract back-to-back clauses
"Payment and Settlement Systems Act, 2007" directions including "Master Direction on Regulation of Payment Aggregators, 2025"	Authorisation, capital/net worth, escrow maintenance, merchant due diligence, storage of payment data in India, tokenisation, settlement timelines, reporting of suspicious merchants	Applies to non-bank PAs, bank PAs, payment gateways, e commerce marketplaces settling funds, sponsor banks holding PA escrows, and merchants routed through PA rails
"Digital Personal Data Protection Act, 2023" including obligations of data fiduciaries and governing consent managers	Lawful processing based on consent or legitimate use, notice, withdrawal, data accuracy, security safeguards, breach reporting to DPB and affected principals, erasure and storage limitation, higher duties	Applies to banks, NBFCs, AAs, PAs, fintech LSPs, cloud and analytics vendors processing personal data on their behalf, and to consent managers who mediate data flows

[17] Ram Prakash Chaubey, "Cybercrime Investigation in India: An Analysis of Digital Evidence and Its Role in Proving Cybercrimes", *available at:* https://www.lawjournals.net/assets/archives/2025/vol7issue3/7067.pdf (last visited on October 31, 2025).

[18] Pavan Duggal, *Indian Cyberlaw & Work From Home* 118 (Notion Press, Chennai, 1st edn., 2020).

	for Significant Data Fiduciaries	
CERT-In Directions dated 28.04.2022 under "Section 70B of the IT Act, 2000" and FAQs	Reporting of 20 listed categories of cyber incidents within 6 hours, log retention in India for 180 days, time synchronisation, information sharing with CERT-In, KYC of subscribers for VPS/VPN, cooperation in investigations	Applies to every entity in the digital banking stack including banks, NBFCs, PAs, AAs, payment gateways, IT service providers, cloud providers and even foreign entities offering services in India
NPCI operating circulars for UPI, RuPay, e-mandates and Aadhaar enabled payment systems[19]	Onboarding standards, dispute and chargeback rules, transaction level risk controls, data localisation and key management, audit requirements,	Applies to member banks, PSPs, TPAPs, PAs integrating with UPI, and to merchant acquirers who route UPI or RuPay
	penalties for SLA breaches	transaction s

Table 1: Key cross-cutting obligations for banks and partners[20]

1.3 ENTITY PERIMETER AND BUSINESS MODELS

Digital banking in India is not confined to traditional scheduled commercial banks. It spans at least seven regulated archetypes and several unregulated or partially regulated participants that plug into the banking system through outsourcing and agency arrangements. Scheduled commercial banks continue to sit at the core because they alone can accept demand deposits without cap, offer the full suite of credit, operate Nostro/Vostro accounts and act as settlement banks for payment aggregators. Around them are built payments banks, small finance banks, NBFCs of various categories, non-bank payment aggregators, NBFC-Account Aggregators, card networks, prepaid issuers and, increasingly, fintech platforms that act as lending service providers, customer acquisition partners or technology service providers. Since 2022, the RBI has reinforced that outsourcing cannot result in a shell bank or a shell NBFC that merely lends its licence, so every digital product that a fintech markets must be tied to a clearly identified regulated entity and must show that the RE retains underwriting, KYC, customer grievance and data protection responsibilities. Business models therefore often combine a licensed bank or NBFC that books the exposure, a fintech LSP that acquires and services the customer, a payment aggregator that collects and settles funds, and an

[19] Account Aggregator Framework, *available at:* https://financialservices.gov.in/beta/en/account-aggregator-framework (last visited on October 28, 2025).

[20] *Supra* note 16.

account aggregator or consent manager that supplies financial information on the customer. This web sits on public rails created by NPCI and is subject to RBI and CERT-In scrutiny. Keeping this perimeter clear is essential for consumer protection as well as for the application of criminal law under the "Bharatiya Nyaya Sanhita, 2023" when digital banking frauds occur, because liability must be traced to the entity that had the duty to verify identity, protect data or monitor transactions.[21]

1.3.1 Scheduled Commercial Banks and Digital Banking Units

Scheduled commercial banks were directed by the RBI's circular dated 7 April 2022 to set up Digital Banking Units as specialised fixed point business units delivering digital banking products and services, with an emphasis on customer experience, cybersecurity, auditability and integration with the bank's core banking system. These DBUs were to offer asset and liability products, services such as opening of accounts, loans, bill payments, fixed deposits, credit cards, and customer grievance redress through digital means, and were to be manned by staff with adequate IT and business knowledge, supported by robust system access and cyber security controls.[22] The purpose was to create uniform digital-first service delivery without compromising prudential norms or KYC standards, and to demonstrate that even public sector banks could provide high quality digital services in smaller centres. DBUs are expected to follow the same KYC Master Direction, to maintain full audit trails for every transaction, to adopt V-CIP or assisted onboarding where appropriate, and to ensure that outsourced IT components meet the RBI's IT Outsourcing Directions. They must also comply with CERT-In's six-hour reporting requirement as incidents affecting a DBU can disrupt core banking access, and with DPDP consent and breach notification provisions because DBUs will store and process large volumes of personal data.

1.3.2 Payments Banks

Payments banks are a specialised class of banks created to advance financial inclusion by accepting demand deposits up to a prescribed limit, issuing ATM/debit cards, enabling domestic remittances through mobile and other channels, and acting as BCs for other banks, while being prohibited from lending and from accepting NRI deposits. Over the years, the RBI has gradually raised the maximum balance per customer to ₹2 lakh, recognising the growth in digital transactions and the need to hold higher operating balances. Payments banks have been critical in onboarding customers into UPI and in acting as settlement banks for wallets and PAs, yet they operate on thin margins and are highly reliant on partnering with full-service banks and technology providers. This makes them especially sensitive to the 2023 IT Outsourcing Directions, to PA and PSS Act requirements on escrow maintenance, and to DPDP and CERT-In compliance because they collect KYC and transactional data at scale but often process it on outsourced infrastructure. Payments banks must also comply with the KYC Master Direction and offer re-KYC through assisted or digital means,

[21] 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).

[22] Establishment of Digital Banking Units (DBUs), *available at:* https://ficci.in/public/storage/sector/Report/22068/RBI_DBU.PDF (last visited on October 30, 2025).

which after the 2025 KYC amendments can be carried out through V-CIP or via business correspondents for periodic updation. Because they interface directly with retail customers, failure in their compliance exposes the system to fraudulent accounts and to offences of cheating, personation or forgery under "Sections 334 to 338 of the Bharatiya Nyaya Sanhita, 2023" and requires proof of electronic records under the BSA.[23]

1.3.3 NBFCs and Fintech Partnerships

Non-banking financial companies have been at the heart of India's digital lending growth because they can move faster than banks in designing and launching products, can leverage fintech front ends for customer acquisition and underwriting, and can enter into FLDG or DLG arrangements to share risk with platform partners. The RBI's Digital Lending Guidelines of 2 September 2022 brought NBFCs squarely under digital conduct norms by requiring that all lending through digital means, including those through LSPs, must be reported to credit information companies, must disclose APR and must ensure that automatic increases in credit limits are not carried out without explicit consent. The June 8, 2023 Guidelines on Default Loss Guarantee in Digital Lending permitted such arrangements but capped the DLG at 5 percent of the loan portfolio and required that the guarantee be invoked only after proof of default, to prevent fintech's from effectively assuming credit risk without being regulated as NBFCs.[24] Subsequent supervisory actions in 2025 have gone further and asked NBFCs not to reduce provisioning by taking credit for fintech provided DLGs, indicating an enforcement trend towards transparency and prudential conservatism.[25] Parallelly, the RBI's "Outsourcing of IT Services Directions, 2023" and its 2024 operational resilience note have made it clear that NBFCs must have board approved policies, due diligence on service providers, performance monitoring, data localisation and exit strategies, and that they must ensure that fintech partners do not store, modify or misuse customer data in violation of DPDP or RBI rules. This rebalancing has significant implications for business models that previously relied on aggressive customer data monetisation, cross selling or multi-platform data pooling without explicit, revocable consent.

1.3.4 Payment Aggregators and Gateways

Payment aggregators and gateways, which began as purely technological intermediaries to route customer payments to merchants, have become heavily regulated because they now handle large volumes of funds, store sensitive payment data and serve as the public interface for countless digital banking transactions. The RBI's initial 2020 guidelines sought to regulate online PAs, prescribe net worth and escrow norms and prohibit card data storage, but experience showed

[23] The Bharatiya Nyaya (Second) Sanhita, 2023, *available at:* https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/173_2023_LS_Eng1212202342949PM.pdf?source=legislation (last visited on October 29, 2025).

[24] RBI Guidelines On Default Loss Guarantee (DLG) In Digital Lending, *available at:* https://ibclaw.in/rbi-guidelines-on-default-loss-guarantee-dlg-in-digital-lending-dated-08-06-2023/ (last visited on October 26, 2025).

[25] RBI Tightens Default Loss Guarantee Rule; NBFCs To Exclude Cover On Fintech-Sourced Loans, *available at:* https://economictimes.indiatimes.com/industry/banking/finance/rbi-tightens-default-loss-guarantee-rule-nbfcs-to-exclude-cover-on-fintech-sourced-loans/articleshow/121420936.cms (last visited on October 25, 2025).

that these entities also operated in offline contexts, in cross border situations and through complex sub merchant structures. This led to the consolidated "Master Direction on Regulation of Payment Aggregators, 2025" under "Section 18 of the PSS Act, 2007" which now applies to all PAs, whether bank or non-bank, operating in online or physical environments, and requires stringent merchant due diligence, transaction monitoring, settlement discipline, capital adequacy, reporting of suspicious activities and full compliance with data localisation and tokenisation rules. The 2025 directions also reference CERT-In timelines and require PAs to ensure that their service providers and merchants comply with cybersecurity and log retention norms, which pulls e commerce platforms, marketplaces and even small merchants within the ambit of high standard cyber hygiene. By 2025, RBI had also clarified that from 1 August 2025 no entity in the card transaction chain, except card issuers and networks, may store card data, reinforcing the tokenisation first approach. These developments matter to digital banking because PAs are frequently used to collect EMI payments, subscription fees, co lending repayments and even loan disbursements for NBFCs and fintech's, and non-compliance can disrupt these flows across the ecosystem.

1.3.5 Account Aggregators and Consent Artefacts

The Account Aggregator framework introduced by the RBI in 2016 created a new class of NBFCs that provide the service of retrieving or collecting financial information pertaining to a customer from Financial Information Providers and transmitting it to Financial Information Users based on explicit, granular, time bound consent provided by the customer through a standardised artefact. This framework has by 2025 become the backbone for consented data sharing across banks, NBFCs, mutual funds, insurance companies and tax authorities, and is supported by technical standards issued by ReBIT, industry governance by Sahamati, and cross regulator coordination among RBI, SEBI, IRDAI and PFRDA. With the DPDP Act recognising consent managers as accountable entities and prescribing very similar requirements on notice, logging, withdrawal and grievance redress, a strong case has emerged for aligning the AA artefact with DPDP consent so that customers do not have to manage two parallel consent systems. This is reinforced by the fact that AAs are prohibited from storing or using the financial information they transmit and must maintain only the consent logs, a principle also present in the DPDP rules. For digital banking, this harmonisation would permit credit scoring, cash flow-based lending, account portability and personalised product offers without violating privacy, because every data pull would be backed by a revocable, traceable consent that can be produced in court under the BSA in the event of dispute. At the same time, it requires banks and fintech's to integrate their systems with AAs and to ensure that outsourcing or cross border processing of account data does not breach DPDP or RBI outsourcing norms.

Entity type	Licensing/authorisation basis	Key permissible activities	Compliance anchors
Scheduled Commercial Banks	Licensed under "Banking	Full deposit taking,	RBI Act and BR

(including DBUs)	Regulation Act, 1949" and included in the Second Schedule to the RBI Act	lending, digital and branch channels, issuance of cards, PA escrow hosting, participation in AA as FIP/FIU, operation of DBUs	Act directions, KYC Master Direction 2016 (UPD. 2025), IT Outsourcing 2023, DPDP Act 2023, CERT-In 2022, NPCI rules
Small Finance Banks	BR Act licence with specific conditions	Deposits, small ticket loans, digital channels, participation in payment systems	RBI SFB guidelines, KYC Master Direction, DPDP Act 2023, CERT-In 2022
Payments Banks	Licensing guidelines for PBs under BR Act with restrictions	Demand deposits up to ₹2 lakh per	RBI PB guidelines, PSS Act for

		customer, domestic remittances, UPI/AEPS, BC for other banks, distribution of simple products	payment activities, KYC Master Direction, DPDP Act 2023, CERT-In 2022
NBFCs (including digital lenders)	Registered under "Section 45IA of the RBI Act, 1934"	Lending, co lending with banks, digital lending through LSPs, DLG/FLDG within caps	Digital Lending Guidelines 2022, DLG Guidelines 2023, IT Outsourcing 2023, DPDP Act 2023
Payment Aggregators/ Gateways	Authorised under "Section 7/18 of the PSS Act, 2007"	Onboarding merchants, accepting customer funds,	Master Direction on Regulation of Payment Aggregators,

		routing and settlement, tokenisation, offline collections	2025, CERT-In 2022, DPDP Act 2023, card network rules
Fintech Lending Service Providers/technology partners	Not individually licensed but contractually bound to REs and sometimes treated as agents under BNSS	Customer acquisition, underwriting support, collections, data analytics, app interfaces	RBI Digital Lending Guidelines 2022 (obligations through RE), DPDP Act 2023, CERT-In 2022, BSA for record keeping
NBFC-Account Aggregators	NBFC-AA Directions, 2016 under "Section 45L of the RBI Act, 1934"	Consent based retrieval and sharing of financial information,	AA Directions 2016, DPDP Act 2023 for consent management
		maintenance of consent logs	er alignment, CERT-In 2022 for log security

Table 2: Licensing and permissible activities

1.4 ONBOARDING, KYC-AML, AND AADHAAR USE

Digital onboarding is the gateway through which customers, especially first-time users, enter the banking system, so the legal soundness and auditability of onboarding determine the enforceability of subsequent contracts, the ability to report suspicious transactions under the PMLA, and the capability to prosecute fraud or data theft under the BNS and to prove electronic records under the BSA. The "Master Direction-Know Your Customer (KYC) Direction, 2016" as successively amended till August 14, 2025 recognises three broad modes for customer due diligence, namely face to face KYC, non-face to face or OTP based KYC subject to limitations, and Video based Customer Identification Process which the RBI treats as equivalent to face to face if all technical and procedural requirements are met. For digital banking this means that banks, NBFCs, payment banks and PAs that onboard merchants must invest in secure video platforms, liveness detection, geo tagging of sessions, retention of video and photograph records, and periodic independent audits. At the same time, Aadhaar based e-KYC remains a powerful tool, but after the Supreme Court's privacy and Aadhaar decisions it can be used only by entities authorised under the Aadhaar Act or by those permitted by UIDAI/RBI, and even then only for

purposes notified by the Central Government, which pushes banks to maintain alternative KYC journeys for customers who do not wish to use Aadhaar.[26] Given that AML/CFT obligations under the PMLA, 2002 as upheld in 2022 require prompt reporting, freezing and production of records, digital onboarding systems must integrate seamlessly with FIU-IND reporting and with the BNSS provisions on search, seizure and production of electronic documents.[27]

1.4.1 KYC Master Direction and V-Cip

The KYC Master Direction, in its 2023, 2024 and 2025 amendments, clarified that V-CIP is to be treated on par with face to face customer identification provided it is conducted live, with trained officials, through end to end encrypted channels, with randomised questions and with capture of clear images of officially valid documents, and that assisted V-CIP can be used to reach customers in remote locations.[28] It also permitted non face to face onboarding using Aadhaar OTP based e-KYC or equivalent OVDs but mandated that such accounts would be subject to restrictions on balance, transactions and cross border remittances until full KYC is completed. After June 12, 2025, the RBI allowed even greater flexibility by enabling customers to complete KYC through business correspondents and by reducing the friction in periodic updation, yet it repeated that regulated entities must maintain high quality, tamper evident records, conduct risk based re-KYC and monitor for anomalies, especially where onboarding is non face to face.[29] In practice, this requires banks and NBFCs to invest in AI assisted liveness detection, geo fencing, device fingerprinting, and to subject V-CIP platforms to annual system audits and penetration tests, all of which must be documented and made available to RBI inspectors and, if a cyber incident occurs, to CERT-In. Since digital KYC journeys generate and store large volumes of biometric, photograph and document data, DPDP requirements on purpose limitation, retention and data principal access must be coded into these workflows, and any breach must be notified to the DPB and to affected persons. For litigation or investigation, these KYC records will have to be produced as electronic evidence, making "Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023" on admissibility and proof of electronic records directly relevant.

1.4.2 Aadhaar, Privacy and Proportionality

The constitutional recognition of the right to privacy in "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[30], and the subsequent Aadhaar judgment of 26 September 2018, which upheld the Aadhaar Act while striking down or reading down parts relating to private sector use and mandatory linkage, reshape how digital banking in India may rely on Aadhaar for customer onboarding. These rulings require that any use of Aadhaar must meet the tests of legality, necessity and proportionality, must be backed by law, and

[26] Justice K. S. Puttaswamy (Retd.) And Anr. Vs Union Of India And Ors., *available at:* https://indiankanoon.org/doc/91938676/ (last visited on October 24, 2025).

[27] Vijay Madanlal Choudhary And Ors. Vs Union Of India, *available at:* https://indiankanoon.org/doc/14485072/ (last visited on October 23, 2025).

[28] FAQs On Master Direction On KYC, *available at:* https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=3782 (last visited on October 22, 2025).

[29] RBI Simplifies KYC Rules To Allow Face-To-Face, Video And OTP-Based Onboarding For Customers, *available at:* https://economictimes.indiatimes.com/news/economy/policy/rbi-know-your-customer-kyc-rules-customer-onboarding-aadhaar-biometric-norms/articleshow/121797850.cms (last visited on October 31, 2025).

[30] *Supra* note 6.

must respect informed consent and purpose limitation. Digital banking entities therefore cannot indiscriminately mandate Aadhaar authentication for all services but must offer alternative KYC methods, must limit storage of Aadhaar numbers, and must mask or tokenise Aadhaar where retention is necessary. The DPDP Act reinforces this by invalidating any part of consent that is not necessary for the specified purpose and by permitting data principals to withdraw consent with ease, which in turn obligates banks and fintech platforms to design KYC and onboarding journeys that can continue service while respecting such withdrawal. For high value or high-risk accounts, reliance on Aadhaar may still be justified, especially when combined with V-CIP and geo tagged address verification, but such reliance must be documented so that, if challenged before a court or a data protection authority, the bank can show proportionality. Since breaches of Aadhaar or identity data can attract offences under the "Bharatiya Nyaya Sanhita, 2023" concerning forgery of electronic records or cheating by personation using computer resources, digital bankers must ensure that their Aadhaar related processes generate contemporaneous logs, alerts and reports that can be investigated under the BNSS and proved in court under the BSA.

1.4.3 AML under PMLA

Anti money laundering compliance has become more stringent for digital banking after the Supreme Court in "*Vijay Madanlal Choudhary v. Union of India*[31], (2022) 10 SCC 1" upheld the core provisions of the "Prevention of Money Laundering Act, 2002" including search, seizure, arrest, attachment and bail conditions, thereby confirming that reporting entities must maintain meticulous records, file timely suspicious transaction reports and cooperate fully with enforcement agencies. For banks, NBFCs and PAs that rely on purely digital onboarding and transaction processing, this means that their KYC and transaction monitoring systems must be robust enough to detect layering, rapid movement across wallets and accounts, mule account behaviour and use of merchant accounts for personal transfers, and must be able to freeze or report such activity without manual intervention. The RBI's digital lending and PA directions have already tried to eliminate pass through accounts and undisclosed fee deductions, but PMLA enforcement shows that authorities are prepared to look through fintech partnerships and treat the regulated entity as responsible for funds that move through its ecosystem. This calls for integration of AML systems with AA data so that real time cash flow and account ownership can be verified with consent, and for alignment with BNSS provisions on search and seizure of digital evidence, including the requirement to produce logs and electronic documents. It also requires meticulous customer education and secure digital communication so that suspicious transaction confirmations, STR acknowledgements and freeze notices can be served in an admissible form under the BSA.[32]

[31] *Supra* note 7.

[32] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 30, 2025).

Onboarding/KYC mode	Core controls and safeguards	Audit and record requirements
Face to face KYC under KYC Master Direction 2016 (updated 2025)	Physical verification of OVD, live photograph, officer sign off, screening against sanctions and internal watch lists	Maintain scanned copies, officer notes, branch logs, risk rating, periodic re-KYC, DPDP compliant notices and consents
Non face to face/OTP based KYC for small value accounts	OTP to Aadhaar linked mobile or alternate digital identifier, restrictions on balance and transactions, first credit from KYC compliant account, enhanced monitoring for mule patterns	Store OTP logs, IP/device data, transaction flags, periodic upgrade to full KYC, report anomalies to FIU and CERT-In if cyber indicators are present
V-CIP and assisted V-CIP	Live audio video session, geo tagging, liveness and spoofing checks, capture of OVD and customer images, trained officer interaction, secure network, time stamped video storage in India	Retain video and snapshots for period prescribed by RBI and DPDP, maintain audit trails of officer IDs, tamper proof storage, periodic system and VAPT audits, ability to produce electronic record with BSA certificate
Aadhaar e-KYC through authorised KUA/Sub-KUA[33]	UIDAI authorisation, explicit consent, masked Aadhaar storage, alternative KYC on refusal, separation of authentication response from other data, risk-based authentication	Preserve consent artefact, UIDAI audit logs, transaction IDs, DPDP notices, incident reports for any Aadhaar data breach, cooperation with CERT-In and UIDAI audits

Table 3: Onboarding modes vs control requirements

[33] Constitutionality Of Aadhaar: Justice K. S. Puttaswamy (Union Of India) - Judgment In Plain English, *available at:* https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/ (last visited on October 29, 2025).

1.5 DIGITAL LENDING: REGULATORY CONSOLIDATION AND FRICTIONS

Digital lending in India has moved from a permissive and often opaque app-based environment to a rule-heavy, disclosure-driven and bank-anchored ecosystem. The Reserve Bank of India has treated unregulated lending apps, synthetic balance-sheet arrangements and unbacked credit lines as a threat to consumer confidence and to prudential soundness. The shift since September 2022 has been to pull every digital lending journey through a clearly identified regulated entity, insist that money flow only between the bank or NBFC account and the borrower account, and to narrow the space available to purely technological intermediaries that operated without capital, supervision or accountability. The effort created short-term frictions, because many fintech models relied on first-loss guarantees, wallet-based credit top-ups and merchant-led credit funnels. Yet the same effort has created a more legible regulatory perimeter, within which recovery methods can be scrutinised under "Section 106 of the Bharatiya Nyaya Sanhita" on criminal intimidation, borrower communication can be assessed in light of "Section 349 of the Bharatiya Nyaya Sanhita" on cheating-like conduct, and record keeping can be supported by "Section 61 of the Bharatiya Sakshya Adhiniyam" on admissibility of electronic records. The aim is not to slow digital credit, but to make it traceable to a supervised balance sheet and to keep customer consent and cost transparency non-negotiable. This approach responds to the Working Group's concerns on over-lending, fake recovery agents, data scraping and buy-now-pay-later opacity, and it locks the entire market to RBI's ability to examine, to order refunds, and to link any failure to licensing conditions.

1.5.1 Digital Lending Guidelines 2022

The September 2, 2022 guidelines bind every bank, cooperative bank and NBFC to a single principle that all loans, even if sourced through an app or through an LSP, must be sanctioned and disbursed by a regulated entity and must be serviced only between the regulated entity's account and the borrower's account. The guidelines require a Key Fact Statement that discloses the all-in Annual Percentage Rate, recovery channels, grievance officials and information on cooling-off, so that a borrower can exit the digital loan by repaying the principal and proportionate interest without penal charges during a short opt-out window. Every fee that is paid to the lending service provider must be paid by the regulated entity and cannot be netted from borrower disbursements, which shuts down the earlier practice of platforms skimming set-up charges upfront. The rules also insist that all data scraped or collected by the LSP is used only for the stated loan purpose and that such data must be purged once the purpose is met or consent is withdrawn, which keeps the conduct consistent with "Section 5 of the Digital Personal Data Protection Act, 2023" on purpose limitation and "Section 9 of the Digital Personal Data Protection Act, 2023" on data erasure. The cooling-off clause, the audit trail of loan flow, and the compulsion to store documents in systems that RBI supervisors can access, create an evidentiary base that can be produced under the BSA without contest about authenticity or integrity. At the same time, market practice reveals that many LSPs tried to rework their contracts to convert themselves into outsourced service providers, to

avoid direct RBI scrutiny. RBI responded by keeping the liability on the regulated entity absolute, which means the bank or NBFC remains answerable even if the LSP violated disclosure or recovery norms. The framework has therefore redistributed risk from consumers to balance sheets.

1.5.2 Default Loss Guarantee Framework 2023

The June 8, 2023 circular on Default Loss Guarantee brought to the surface an informal practice in which fintech-originators or platform partners promised to absorb first losses on pools sourced for banks and NBFCs. RBI converted this practice into a disclosed, audited and capped arrangement. A DLG can now cover only up to 5 percent of the loan portfolio to which it relates, it must be backed by an enforceable contract, it must be provided in cash deposit, fixed deposit, or bank guarantee form, and once a loss is invoked the guarantee cannot be replenished. This design prevents thinly capitalised fintech's from writing open-ended guarantees and dressing up credit risk. The circular openly links itself to the 2022 digital lending guidelines and allows DLGs only when the underlying loans are otherwise compliant. For NBFCs intending to rely entirely on DLG comfort, RBI signalled that capital and provisioning norms will tighten in 2025 so that risk is not transferred to entities without minimum owned funds and without long term skin in the pool. That tightening lines up with the later co-lending directions, which require a 10 percent on-book share to be retained by the originator, and it means that a DLG cannot be the only form of risk retention. For accounting purposes, banks will have to examine whether DLG-linked pools need higher expected credit loss provisioning since the guarantee cannot be reinstated. For contractual purposes, the DLG provider must file a statutory auditor's certificate, which brings professional liability into the picture and locks the arrangement to domestic jurisdiction, reducing the risk of foreign guarantee vehicles escaping scrutiny.[34]

1.5.3 BNPL and PPI-Credit Line Prohibition

The June 20, 2022 clarification to authorised PPI issuers that PPIs cannot be loaded through credit lines stopped several BNPL constructs that used a wallet or card front-end to deliver an underlying credit drawdown. RBI saw that these models could replicate a credit card without being subject to card issuance rules, minimum capital standards, or fair practice codes. By directing issuers to stop the practice immediately, RBI ensured that every wallet or PPI top-up reflected real money and not synthetic credit. BNPL players then tried to migrate to co-lending or to term loans with explicit disbursements, but the earlier embedded and invisible credit experience was altered. From a legal standpoint this move grounded PPI transactions in the Payments and Settlement Systems Act and made unauthorised credit-loading a compliance breach that could trigger supervisory action even without any borrower complaint. It also protected consumers from compound charges by merchants, since any credit supply now had to disclose rate, tenor and recovery. When such loading happens in spite of the bar, it becomes easier to link the act to

[34] Guidelines on Default Loss Guarantee in Digital Lending, *available at:* https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3592 (last visited on October 28, 2025).

wrongful gain under "Section 317 of the Bharatiya Nyaya Sanhita" and to misrepresentation of services under "Section 338 of the Bharatiya Nyaya Sanhita", while the electronic records of top-ups remain admissible through "Section 63 of the Bharatiya Sakshya Adhiniyam". The market had to re-engineer BNPL into proper small-ticket credit under a regulated entity, with periodic reporting to RBI's CRILC and CIC systems.[35]

1.5.4 Co-lending and Risk Retention

The 2025 co-lending directions completed the consolidation by stating that every party to a co-lending arrangement must keep at least 10 percent of every individual loan on its own books and must record that share within 15 days of disbursement. The directions extended co-lending beyond priority sector lending and linked them to general credit supply, which means most digital-first partnerships between banks and NBFCs now come under one harmonised rulebook. The directions also repeated the 5 percent cap on DLGs, but made clear that this cap operates only on the originating regulated entity and cannot be used by third parties to provide synthetic over-collateralisation. Alignment of incentives is achieved because an originator that retains 10 percent of every loan will not chase unsustainable growth through aggressive LSPs. Alignment is also achieved because all borrower-facing documents must disclose both lenders, contact details and dispute resolution mechanisms, which will later tie into the Ombudsman scheme. These directions sit well with BNSS provisions on service of summons and notices, since the borrower will have two clear counterparties on record. From 1 January 2026, co-lending will therefore produce a cleaner risk distribution, with RBI able to see which entity failed to classify, which one breached KYC, and which one misreported default to CICs.[36]

1.6 DATA GOVERNANCE, TOKENISATION AND LOCALISATION

Data governance in digital banking in India now operates on a dual axis. At the horizontal level lies the "Digital Personal Data Protection Act, 2023", which treats banks as data fiduciaries holding large volumes of financial personal data and requires consent, purpose limitation, erasure, security safeguards and grievance redress. At the sectoral level lie RBI's master directions, circulars on payment system data, tokenisation and card-on-file, and IT governance directions that treat the same banks as regulated entities required to ensure confidentiality, integrity and availability of customer data for supervisory access. The friction arises because banking business often runs on analytics, cross-selling and outsourced processing. The legal position today is that every such use must be covered by a lawful purpose, the data must predominantly stay in India in respect of payments, and customers must be able to see, correct and erase their data unless retention is necessary for law enforcement, tax or anti-money laundering purposes.

[35] RBI Guidance on Loading of PPIs Through Credit Lines, *available at:* https://www.cyrilshroff.com/wp-content/uploads/2022/08/Insight-Newsletter.pdf (last visited on October 27, 2025).

[36] Ayush Chowdhury, Yash Jain, "Analysis of RBI Co-Lending Arrangements Directions, 2025", *available at:* https://corporate.cyrilamarchandblogs.com/2025/09/analysis-of-rbi-co-lending-arrangements-directions-2025/ (last visited on October 26, 2025).

1.6.1 DPDP Implementation Themes for Banks

The DPDP Act sets out notice-and-consent as the primary gateway to processing, so banks have to articulate to customers why each data field is being collected and how it will be used. For digital banking, this applies not only to account opening but also to mobile app telemetry, location capture, device fingerprinting, behavioural scoring and video-KYC recordings. “Section 5 of the Digital Personal Data Protection Act, 2023” on purpose limitation, “Section 7” on legitimate uses and “Section 13” on grievance redress together require banks to run consent dashboards or to appoint consent managers, and they must respond within the timelines to be notified by the central government. Since RBI already requires a grievance officer and a 30-day resolution period for customer complaints, banks will have to run parallel but coordinated channels to satisfy both regulators. When banks share account or transaction data with fintech partners, they must ensure that such sharing is either consented or is covered under a legitimate use such as compliance with “Section 39 of the Bharatiya Nagarik Suraksha Sanhita” on production of documents to police or under PMLA duties. The multiplicity of norms means the weakest link will determine liability - a failure to erase telematics after loan closure, or a failure to record consent for device binding, can trigger action both from the Data Protection Board and from RBI. Banks will also have to align DPDP retention requirements with BSA evidentiary needs, so that data is kept for the statutory period and can be produced in court trials relating to digital fraud, while privacy is protected for marketing data that has outlived its purpose.

1.6.2 Storage of Payment System Data in India

The April 6, 2018 directive required every payment system operator to store, in India, the entire data relating to payment systems they operate, including full end-to-end transaction details, payment instructions, originator and beneficiary information, and to make this data available to RBI for supervision. RBI later clarified in June 2019 that data could be processed abroad, but a complete copy had to be stored in India and that system providers must submit board-approved system audit reports. This directive responds to national security and supervisory concerns and has been repeatedly enforced in licensing decisions and in evaluations of big tech payment entities. For digital banking, this means that even if a bank uses a global payment gateway, cloud or switch, it must ensure data localisation through contractual clauses and technical controls. Localisation strengthens law enforcement because investigation agencies operating under BNSS can obtain payment records swiftly without resorting to mutual legal assistance, and banks can satisfy their obligation to produce records under BSA. Over time, RBI has extended the spirit of this directive to UPI, card networks, white label ATMs and cross-border inwards, ensuring that anything that touches the Indian payment system is discoverable in India. Non-compliance can produce restrictions similar to those imposed on

Paytm Payments Bank where RBI cited persistent supervisory concerns.[37]

1.6.3 Tokenisation and Card-On-File

Tokenisation policy enabled customers to pay online without exposing the actual card number and to let the merchant or device use a token issued by the card network and the bank. RBI's 2021 to 2023 updates instructed merchants to purge stored card data by September 30, 2022 and to rely on issuer-enabled CoFT (card on file tokenisation). This shift reduced card data theft, limited merchant-level breaches and placed liability on issuers to validate additional factor authentication. Tokenisation also allowed device-based payments through wearables, IoT devices and contactless channels. For banks, the main regulatory load is to secure token vaults, to obtain explicit customer consent for each token, and to ensure that recurring mandates over Rs. 5,000 follow additional factor authentication even when tokenised. Since DPDP requires purpose-specific consent, banks must link tokenisation consent to the payment use case and offer revocation. Since RBI wants international card-not-present transactions to carry AFA from April 1, 2026, tokenisation becomes the baseline security feature on which stronger authentication will ride, including for cross-border e-commerce.[38]

1.7 CYBERSECURITY, OUTSOURCING AND OPERATIONAL RESILIENCE

Digital banking scale depends on uninterrupted, secure and auditable technology. RBI has learned from repeated outages, card network downtimes and cooperative bank cyber incidents that resilience cannot be left to market practice. The current approach is to lay down baseline cyber requirements, require board-approved outsourcing policies, and to connect operational risk management with third-party concentration monitoring. RBI's stance is supported by national cybersecurity rules, especially CERT-In's six-hour reporting rule issued under "Section 70B of the Information Technology Act, 2000", which now runs parallel to RBI's incident reporting requirements. For banks, this creates a tight timeline for disclosure and for forensic preservation of logs inside India, and it brings in BNSS provisions on production of documents in criminal inquiries related to hacking or data theft.[39]

1.7.1 RBI Cyber Security Framework for Banks

RBI's cyber framework for banks requires a board-level information security policy, a Cyber Crisis Management Plan, periodic vulnerability assessments and penetration tests, real-time security information event management, and reporting of unusual cyber incidents to the regulator. As digital channels have grown, RBI has also pushed for secure application development, customer awareness and multi-factor authentication requirements. The CCMP expectation is very precise - banks must rehearse response, keep a list of critical services, have

[37] Payment And Settlement Systems - Storage Of Payment System Data (FAQs), *available at:* https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995 (last visited on October 28, 2025).

[38] Device Based Tokenisation – Card Transactions, *available at:* https://www.rbi.org.in/commonman/English/Scripts/FAQs.aspx?Id=2917 (last visited on October 25, 2025).

[39] Master Direction On Outsourcing Of Information Technology Services, *available at:* https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12486 (last visited on October 27, 2025).

alternate channels ready, and restore services within tolerances fixed by the board. After the HDFC Bank outages in 2020, RBI demonstrated that failure to maintain such standards can lead to a freeze on new digital products and on credit cards. The cyber framework now sits alongside the 2024 operational resilience guidance, creating a single continuum from prevention to recovery. Since customer data is a key asset, this framework works in tandem with DPDP security safeguards and with RBI data localisation rules, meaning that a breach involving payments data must be reported both to RBI and to CERT-In, and logs must be stored in India for 180 days as required by CERT-In.[40]

1.7.2 Outsourcing of IT Services Directions 2023

The 2023 directions on outsourcing of IT services apply to banks, NBFCs, credit information companies and other regulated entities, and they make it clear that outsourcing does not reduce the obligations of the regulated entity to its customers or to RBI. Every bank must have a board-approved policy defining materiality thresholds, due diligence standards, model contract clauses, audit and inspection rights, termination and exit strategies, and data protection covenants. Contracts must provide RBI and the bank unrestricted access to data, logs, business premises and subcontractors, even when the service is on cloud. This means that a bank cannot excuse delayed reporting to CERT-In on the ground that its cloud provider is offshore. The directions extend liability to subcontractors, so the chain of accountability reaches the smallest outsourced operation. They also tie into payment data localisation and to DPDP's requirement that data fiduciaries ensure comparable levels of data protection in onward transfers. In practice this forces banks to maintain an accurate register of all IT and fintech vendors, test their incident response plans, and reconsider concentration where a single cloud or a single switching provider supports critical payment workloads.

1.7.3 Operational Risk and Resilience Guidance 2024

On 30 April 2024 RBI issued an updated Guidance Note on Operational Risk Management and Operational Resilience to all regulated entities, expanding the earlier 2005 guidance and absorbing many of the Basel Committee principles. The note requires banks and NBFCs to integrate ICT risk, cyber risk, third-party risk, business continuity and payment system dependencies into a single enterprise operational risk framework. Boards have to set impact tolerances for critical services such as mobile banking, UPI on-boarding, credit card issuance and loan management systems, and senior management must test whether the organisation can recover within those tolerances. The note also asks entities to manage intragroup and affiliate service dependencies, something that became important when Paytm Payments Bank faced restrictions in 2024 and had to isolate activities and customer funds. The guidance is flexible on methods, but non-negotiable on outcomes - financial entities must continue to provide critical

[40] Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, *available at:* https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited on October 24, 2025).

services with minimal disruption and must document risk ownership. This gives RBI leverage to impose business curbs when IT audits show recurring deficiencies, as seen in the Kotak Mahindra Bank order of April 24, 2024.[41]

1.7.4 CERT-in's Six-Hour Rule and Coordination

CERT-In's directions of April 28, 2022 introduced a six-hour window for reporting a wide universe of cyber incidents, including targeted scanning, DDoS, ransomware, data breaches, and attacks on AI systems. The directions require entities to synchronise time, maintain logs in India for 180 days, and to respond to CERT-In's demands for information. Banks and payment companies already report cyber incidents to RBI under its cyber security framework, so this created practical overlaps. The prudent approach has been to file reports with both RBI and CERT-In, often within the shorter CERT-In timeline, and to keep an internal log that can be produced to both authorities. Since CERT-In acts under the IT Act while RBI acts under the RBI Act and the Payment and Settlement Systems Act, banks have to be careful about disclosure of personal data and must rely on "Section 8 of the Digital Personal Data Protection Act, 2023" which permits disclosure for compliance with any law in force. A failure to report can attract action from both regulators, and material incidents can also become a basis for RBI to impose operational restrictions, just as in the HDFC and Kotak cases.

1.8 CONSUMER PROTECTION AND DISPUTE RESOLUTION

Digital banking has brought millions of first-time customers into formal finance, so RBI has had to build a dispute resolution system that is fast, inexpensive and familiar. The policy choice has been to unify redress across banks, NBFCs and payment system participants, to require online dispute resolution for payment failures, and to harden authentication so that liability for fraud is easy to determine. This consumer protection layer works with DPDP grievance rights, with banks' duty to record and evidence transactions under BSA, and with penal consequences under BNS for unauthorised access, cheating or criminal intimidation in recovery. For customers, the existence of a free Ombudsman route backed by enforceable RBI directions restores trust when digital services fail.[42]

1.8.1 RBI Integrated Ombudsman Scheme 2021

The RB-IOS 2021 merged three earlier Ombudsman schemes and brought under one roof complaints against banks, NBFCs, payment system participants and credit information companies. It removed jurisdictional limitations and allowed complaints to be filed online, through email or in writing, with no charge to the complainant. A customer can approach the Ombudsman if the regulated entity has not replied within 30 days or has rejected the complaint. The scheme defines deficiency in service broadly enough to cover failed digital transactions, wrongful debits, unauthorised card use, refusal to

[41] Guidance Note On Operational Risk Management And Operational Resilience, *available at:* https://www.pdicai.org/Docs/RBI-2024-25-31_15202415340467.pdf (last visited on October 29, 2025).

[42] 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).

close accounts, credit reporting errors and mis-selling through apps. For digital banking, this means that even when the problem arises from an outsourced service or from a co-lending partner, the customer can proceed against the principal regulated entity. RBI has backed the scheme with internal ombudsman directions in 2023, requiring large entities to have an internal appellate mechanism before the matter goes outside. This design spreads accountability and gives RBI a comprehensive dataset of recurring issues, which it can match with supervisory findings.

1.8.2 ODR for Digital Payments

The August 6, 2020 circular on Online Dispute Resolution for digital payments created a rules-based, system-driven mechanism for resolving failed UPI, IMPS, card and wallet transactions. RBI made it compulsory for authorised payment system operators to put such a system in place by January 1, 2021 and to provide access to their participants. Over time RBI has been extending ODR to more transaction categories so that customers need not visit branches or call centres for digital failures. This sits well with digital lending too, because many loan disbursements and repayments ride on UPI and card rails. ODR captures failure data and timeliness of refunds, allowing RBI to spot entities that use float or delay reversals. Since ODR is online, records are readily available for production under BSA when disputes escalate to consumer courts or criminal complaints. A bank that does not integrate with ODR risks being seen as non-cooperative and can face restrictions, just as entities with repeated IT lapses have faced.[43]

1.8.3 Authentication and Fraud Controls

RBI has long required two-factor authentication for domestic card-not-present transactions and has gradually increased the AFA-exempt limit for contactless payments to Rs. 5,000 to support small-value usage. With fraud patterns changing, RBI issued draft and then final directions in 2024-2025 on alternative authentication mechanisms, including for cross-border card-not-present transactions, and from April 1, 2026 most digital payment transactions will need at least two distinct factors unless exempted. This future-dated regime is being reported in the financial press and in The Times of India because it will affect e-commerce, OTT and card-on-file merchants. The purpose is to reduce liability disputes and to harmonise domestic and cross-border security. For banks, this means upgrading customer authentication, monitoring mule accounts, and linking fraudulent behaviour to "Section 316 of the Bharatiya Nyaya Sanhita" on dishonest misappropriation, so that law enforcement can act. Strong authentication also supports DPDP by ensuring that only authenticated principals exercise consent or erasure rights.[44]

1.9 JURISPRUDENCE AND RECENT ENFORCEMENT

Indian jurisprudence on digital banking has so far turned on privacy, proportionality of RBI actions, the legitimate use of Aadhaar for KYC, and the

[43] Online Dispute Resolution (ODR) System For Digital Payments, *available at:* https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=3194 (last visited on October 26, 2025).

[44] Card Not Present Transactions - Relaxation In Additional Factor Of Authentication For Payments Upto ₹2000/- For Card Network Provided Authentication Solutions, *available at:* https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=2067 (last visited on October 25, 2025).

breadth of preventive regimes such as PMLA. These decisions supply constitutional and administrative law guardrails around RBI's otherwise wide powers under the RBI Act and PSS Act. When read with recent supervisory actions on HDFC Bank, Kotak Mahindra Bank and Paytm Payments Bank, they show that courts will demand reasonableness and tailored measures, but they will also recognise RBI's power to protect the system from technology and compliance lapses.

1.9.1 Justice K.S. Puttaswamy v. Union of India,

In the case of *Justice K.S. Puttaswamy v. Union of India*[45], the Supreme Court was faced with the question whether the Constitution of India recognises a fundamental right to privacy that binds the State in all its actions. The Court assembled a nine-judge bench because earlier decisions such as M.P. Sharma and Kharak Singh had cast doubt on privacy. The bench held unanimously that privacy is a fundamental right contained in Part III, sourced in the guarantees of life and personal liberty under Article 21 and in the freedoms under Article 19, and that it covers spatial privacy, informational privacy and decisional autonomy. The judgment took note of the rise of big data, profiling and surveillance, and it recorded that in a modern digital economy the collection and use of personal data by both State and non-State actors can affect dignity. The Court stated that any restriction on privacy must satisfy legality, legitimate aim, proportionality and procedural safeguards. Though the case did not decide Aadhaar, it made it clear that future schemes involving biometric data, financial accounts or identity-linked subsidies would have to be tested against these four steps. For banking, the decision laid the foundation for challenging indiscriminate sharing of customer data, bulk KYC requirements that are not backed by law, and blanket mandates to deposit financial data with private vendors. It also supplied a constitutional basis for the later DPDP Act, because the Act's structure of consent, purpose limitation and grievances mirrors the proportionality and procedural safeguard requirements in the judgment.[46]

1.9.2 K.S. Puttaswamy (Aadhaar-5j.) v. Union of India,

In the case of *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*[47], the Constitution Bench examined the Aadhaar Act, 2016 and the entire architecture of unique identification built on biometric authentication. The Court upheld Aadhaar for State subsidies, benefits and services funded from the Consolidated Fund of India, holding that the legitimate aim of targeted delivery and plugging of leakages was satisfied, and that Aadhaar's use in this limited field was proportionate because of oversight and grievance mechanisms. At the same time the Court struck down or read down provisions that allowed private entities like banks and telecom companies to insist on Aadhaar authentication for their own purposes, finding that such use was not backed by sufficient state interest and could lead to profiling. Sections that enabled long retention and wide sharing of authentication data were also curtailed. For digital banking this meant that

[45] (2018) 1 SCC 809.

[46] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 176 (HarperCollins, Noida, 1st edn., 2018).

[47] (2019) 1 SCC 1.

banks could not make Aadhaar the only route for KYC unless a law or RBI regulation specifically permitted it, and they had to offer alternative OVDs. It also meant that Aadhaar based e-KYC done through third-party BCs or fintech's had to respect purpose limitation and storage controls. The judgment therefore helped shape subsequent RBI KYC Master Directions, the video-KYC framework, and the data minimisation practices that DPDP later codified. Banks can still rely on Aadhaar for DBT-linked accounts or where government schemes demand it, but they cannot harvest Aadhaar numbers for profiling or marketing.

1.9.3 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*[48], the Supreme Court dealt with the RBI circular of April 6, 2018 that directed entities regulated by RBI not to deal in or provide services for virtual currencies. The petitioners argued that RBI's measure had wiped out the business of exchanges even though virtual currencies were not illegal in India. The Court acknowledged that RBI has very wide powers to regulate the financial system and that it can issue preventive circulars to protect payment systems and banking channels from reputational, prudential and AML risks. The Court also noted that RBI had consulted government departments and had repeatedly warned about consumer and market integrity risks. Yet the Court applied the doctrine of proportionality and found that RBI had not shown any actual harm from exchanges' access to banking channels. Since the circular had a serious impact on the right to carry on trade, it could not be justified without evidence of such harm. The Court therefore set aside the circular, but it carefully stated that if RBI, on the basis of fresh material, felt such regulation or prohibition was needed, it could act again. For digital banking the message was that RBI must tailor its restrictions, record reasons and keep its measures proportionate, but that its preventive and supervisory jurisdiction over regulated entities would be upheld. This is the same stance visible in later enforcement where RBI did not cancel licences but froze certain digital activities until technology deficits were cured.

1.9.4 Vijay Madanlal Choudhary v. Union of India,

In the case of *Vijay Madanlal Choudhary v. Union of India*[49], the Supreme Court examined wide-ranging challenges to amendments to the Prevention of Money Laundering Act, 2002, including the reverse burden of proof, arrest and search powers of the Enforcement Directorate, and the width of the definition of proceeds of crime. The Court upheld the core provisions, holding that money laundering is a serious offence with transnational dimensions and that Parliament was competent to create a stringent regime. The Court recognised that PMLA proceedings are distinct from the predicate offence and that the ECIR need not be supplied like an FIR. For digital banking this judgment had immediate consequences. Banks and fintech-linked NBFCs have to treat suspicious digital transactions, mule accounts, cross-border card frauds and wallet abuses seriously, report them promptly as STRs, and maintain records for ten years. Since many digital lending and payment

[48] MANU/SC/0264/2020.

[49] *Supra* note 7.

models rely on rapid onboarding and minimal documentation, the PMLA posture approved in this case demands that KYC be strong, that beneficial ownership be verified, and that entities cooperate fully with FIU-IND. The decision also supports RBI when it asks payment banks or fintech's to ring-fence operations, because any weakness in KYC and monitoring can lead to laundering through those channels.[50]

1.9.5 Supervisory Actions Illustrating Tech-Risk Oversight

RBI's action against HDFC Bank in December 2020, prompted by repeated outages and data centre issues, led to a ban on new digital launches and on issuing new credit cards, a serious commercial setback for India's largest private bank. The restrictions remained until March 2022 when RBI was satisfied about remediation and issued a letter lifting all curbs. This demonstrated that RBI would use business restrictions, not only monetary penalties, to enforce technology standards.[51] In April 2024, RBI imposed similar but narrower curbs on Kotak Mahindra Bank, barring it from onboarding new customers through online and mobile channels and from issuing new credit cards because of deficiencies in IT risk management and information security governance revealed in 2022-23 inspections. The bank could serve existing customers but had to fix its systems and submit to an external audit. This mirrored the pattern established in HDFC Bank's case and communicated to the market that size would not shield entities from tech-governance discipline.[52] In January 2024 and through FAQs of February 16, 2024, RBI directed Paytm Payments Bank to stop accepting deposits, credit transactions and top-ups after March 15, 2024, because of persistent non-compliances and supervisory concerns. Customers could only use existing balances, receive refunds and cashbacks, and close wallets with transfer of balance to other banks. This action, widely covered in the media, demonstrated RBI's resolve to contain risks from payment banks that failed to ring-fence customer funds and to maintain accurate data in India.[53] Together, these actions show an enforcement philosophy that is proportionate, technologically informed and customer-centric, fully consistent with the Supreme Court's approach in the IAMAI case, and they give digital banks a clear warning that business continuity and IT governance are now part of core prudential compliance.

1.10 EMERGING ISSUES

Digital banking continues to expand into AI-driven credit, embedded finance and CBDC-linked wallets. Future regulatory work will focus on the following.

1. AI credit scoring transparency for REs and auditability of models used by LSPs.

[50] Atul Singh, "Data Protection: India in the Information Age", 53 *Journal of the Indian Law Institute* 80 (2011).

[51] RBI Lifts All Restrictions On HDFC Bank's New Digital Launches, *available at:* https://mas360.moneylife.in/article/rbi-lifts-all-restrictions-on-hdfc-bank-s-new-digital-launches/3989.html (last visited on October 24, 2025).

[52] RBI Cracks Down On Kotak Mahindra Bank; Bars Onboarding New Customers Through Online, Mobile Banking And Issuing New Credit Cards, *available at:* https://www.moneycontrol.com/news/business/rbi-bars-kotak-mahindra-bank-from-onboarding-new-customers-through-online-mobile-banking-issue-new-credit-cards-12707215.html (last visited on October 23, 2025).

[53] 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).

2. Cross-border data flows for global merchant acquiring under DPDP and RBI localisation.
3. Third-party wallet operators' access to UPI Lite and fraud liability allocation.
4. CBDC-Retail integration with existing KYC and BNSS reporting duties.
5. Quantum-safe cryptography requirements for payment system operators.
6. Sector-wide cyber tabletop exercises tying RBI, CERT-In and FIU-IND.
7. Harmonisation of co-lending with SRO-led fintech governance codes.
8. Dynamic 2FA standards for wearables and IoT banking devices.
9. Platform neutrality rules for big tech-run superapps offering credit.
10. Supervisory colleges for large fintech groups with NBFC arms.

1.11 CONCLUSION

India's digital banking stack is now governed by a dense but increasingly coherent mesh of sectoral and horizontal rules. On the sectoral side, RBI has clarified the perimeter of digital credit and payments: the 2022 Digital Lending Guidelines re-anchored every digital loan to a supervised balance-sheet with end-to-end fund-flow traceability and mandatory Key Fact Statements, while the 2023 DLG circular capped first-loss sharing to prevent thinly capitalised platforms from warehousing risk off-balance-sheet.[54] The Payment Aggregator regime was consolidated in 2025, extending obligations to physical acquiring, strengthening merchant due diligence, settlement discipline, and reiterating data-on-soil requirements, complementing RBI's 2018 storage directive.[55] Horizontally, DPDP 2023 reframes banks, NBFCs, PAs and AAs as data fiduciaries - reinforcing consent, purpose limitation, security safeguards and breach notification - and sits alongside CERT-In's six-hour incident reporting and log-retention obligations.[56] Consumer protection is carried by an integrated ombudsman with a common intake and by online dispute resolution (ODR) for failed digital payments; together these tools operationalise fast, evidence-ready redress that dovetails with BSA admissibility of electronic records.[57] Finally, RBI's 2024 guidance on operational risk and resilience links third-party/ICT risk to board-set impact tolerances, creating enforcement leverage when outages or governance gaps persist.[58]

The enforcement trajectory confirms this shift from prescriptive checklists to outcomes: HDFC Bank's 2020–22 curbs, Kotak Mahindra Bank's April 2024 restrictions, and Paytm Payments Bank's 2024 constraints show RBI's willingness to use business limits to remedy IT, governance and perimeter risks without necessarily cancelling licences.[59] This regulatory posture has advanced

[54] *Supra* note 10.

[55] Master Direction On Regulation Of Payment Aggregator (PA), *available at:* https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896 (last visited on October 31, 2025).

[56] *Supra* note 2.

[57] The Reserve Bank - Integrated Ombudsman Scheme, 2021, *available at:* https://www.rbi.org.in/CommonPerson/english/Scripts/PressReleases.aspx?Id=3340 (last visited on October 30, 2025).

[58] Guidance Note On Operational Risk Management And Operational Resilience, *available at:* https://www.fidcindia.org.in/wp-content/uploads/2019/06/RBI-PRESS-RELEASE-OPERATIONAL-RISK-MANAGEMENT-30-04-24.pdf (last visited on October 28, 2025).

[59] Akash Podishetti, "RBI Finally Lifts All Curbs on HDFC Bank, Including New Digital Launches", *available at:* https://www.livemint.com/industry/banking/rbi-finally-lifts-curbs-on-new-digital-launches-of-hdfc-bank-11647076803820.html (last visited on October 23, 2025).

inclusion (via V-CIP, assisted KYC, BC-enabled re-KYC) while curbing opaque BNPL/top-up constructs through tokenisation, AFA and PPI credit-line prohibitions, and by bringing DLGs into a disclosed, auditable cap.[60] Yet frictions remain: overlapping reporting lines to RBI/CERT-In/NPCI, partial misalignment between DPDP consent artefacts and the AA framework, and evidence-chain expectations under BSA that are not always embedded in vendor contracts. The way forward is architectural: (i) statutory codification of key digital directions under the PSS Act; (ii) inter-regulatory, schema-driven incident-reporting rails capable of producing BSA-compliant artefacts; (iii) harmonised consent/withdrawal across AA and DPDP; and (iv) risk-tiered KYC that preserves automation for low-value flows but demands stronger auditability and subcontractor visibility for higher-risk products. These measures would lower compliance noise without diluting prudential or consumer outcomes, and would better align India's public digital infrastructure with a maturing, supervised market for embedded finance.

1.12 SUGGESTIONS

In examining the contemporary legal and regulatory challenges in India's digital banking landscape, the following actions are recommended.

1. Unify consent artefacts across AA and DPDP. MeitY and RBI should publish a joint technical standard mapping AA's consent handles to DPDP-compliant notices, withdrawal and logging semantics. Mandate all FIPs/FIUs to accept a DPDP-compliant AA token as sufficient legal basis, with APIs for revocation that cascade to downstream processors within T+1. Require consent dashboards in banking apps to display active AA mandates with one-click withdraw, and obligate REs to propagate withdrawals to vendors via contractually enforceable SLAs. Conduct a six-month industry migration with sandbox certification.
2. Create an inter-regulatory cyber/incident rail. Establish a single JSON schema and gateway that fans out to RBI, CERT-In and (where relevant) NPCI, preserving six-hour first-notice timelines and BSA-ready hash-chained evidence packages. Require REs/PAs to maintain a live subcontractor register and attest that log-retention and time-sync extend to fourth parties. Run semi-annual sector-wide tabletop exercises covering payments, lending, and AA data pulls, with after-action obligations tracked by supervisors Publish anonymised heatmaps of incident typologies and remediation timeliness.
3. Statutorily anchor digital directions under the PSS Act. Amend Section 18/7 to explicitly recognise aggregators (online and physical), tokenisation, data localisation, and ODR mandates, reducing reliance on ad-hoc circulars. Introduce a graded penalty ladder tied to merchant due-diligence failures and settlement-breach severity. Require machine-readable disclosure of escrow breaks and settlement timelines via a standard PA

[60] *Supra* note 26.

transparency report. Provide safe harbours for PAs that demonstrate proactive merchant off-boarding and STR escalation.

4. Make tiered-KYC truly proportionate. Notify a three-tier framework: nano (wallets/UPI Lite), basic (restricted accounts), and full KYC-each with clear limits, re-KYC cadence, and uplift triggers. Permit assisted V-CIP and BC-led periodic updation universally, but require enhanced liveness, device binding, and geotagging for high-risk tiers. Mandate CKYCR round-trips and dedupe checks before account activation; failed dedupe must trigger manual escalation. Require annual third-party audits of V-CIP platforms, with findings shared with RBI.
5. Harden outsourcing chain transparency. Compel REs/NBFCs to maintain an auditable "flow-down" annexure in every contract that binds subcontractors to RBI access, DPDP compliance, log-on-soil, and six-hour reporting. Introduce a critical-services register with board-approved impact tolerances and exit plans per service. Require quarterly CERT-In-empanelled audits for material vendors and publish summary scores to boards and supervisors Cap single-vendor concentration for critical payment workloads or require compensating controls tested in failovers.
6. Close gaps in digital lending conduct. Standardise the Key Fact Statement (KFS) in a machine-readable schema with an APR calculator embedded and mandatory in-app recall. Enforce fund-flow purity with reconciliation APIs that reject LSP pooling attempts and auto-flag off-KFS charges. Require public disclosure of invoked DLGs by pool-vintage and loss-timing; prohibit replenishment and ensure appropriate ECL provisioning at the originator. Tie recovery conduct to verifiable, recorded channels with auditable consent trails.
7. Operational resilience by design. Mandate board-set impact tolerances (RTO/RPO) for mobile banking, UPI onboarding, card issuing, loan servicing, and ODR, with quarterly severe-but-plausible scenario tests. Require REs/PAs to publish customer-facing uptime dashboards, backed by auditor-certified metrics. Link repeated tolerance breaches to targeted business restrictions and remediation milestones. Embed resilience requirements into cloud contracts, including sovereign-support clauses for data and log access.
8. Align tokenisation and cross-border CNP authentication. Enforce "no storage beyond issuer/network" across the chain and require token life-cycle logs to be DPDP-compliant and exportable for BSA evidence. For cross-border CNP, mandate at least two distinct authentication factors or network-level risk controls with explicit customer opt-ins. Require merchants and PAs to display token-status and revoke options at checkout. Penalise repeat non-compliance with acquiring-level sanctions.
9. Evidence-ready by default. Issue a joint RBI–MHA note translating BSA sections on electronic records into concrete

banking artefacts (V-CIP packages, KFS hashes, consent logs, PA settlement files). Require hash-stamping and time-stamping (IST-synced) for all customer-facing artefacts and operational logs, with retention schedules that reconcile PMLA, DPDP and tax rules. Prescribe a standard "BSA certificate" template for production in courts. Test evidentiary readiness during supervisory inspections through sample "drills".

10. Supervision of fintech groups and PAs at scale. Constitute supervisory colleges for large fintech groups with NBFC/PA arms, sharing findings across sectoral regulators Make "fit-and-proper" and capital buffers dynamic-scaling with merchant count, cross-border flows, and complaint ratios. Require SRO-style conduct codes for LSPs/collectors, with certification tied to RE onboarding. Publish comparative heatmaps (merchant vetting lag, ODR timeliness, dispute reversal rates) to drive market discipline.

BIBLIOGRAPHY

Books:

- N S Nappinai, Technology Laws Decoded (LexisNexis, Gurgaon, 1st edn., 2017).
- Nandan Nilekani, Viral Shah, Rebooting India: Realizing a Billion Aspirations (Penguin Books, New Delhi, 1st edn., 2015).
- Pavan Duggal, Indian Cyberlaw & Work From Home (Notion Press, Chennai, 1st edn., 2020).
- Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins, Noida, 1st edn., 2018).

Statutes:

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act No. 18 of 2016)
- 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 Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- 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:

- Atul Singh, "Data Protection: India in the Information Age", 53 Journal of the Indian Law Institute 80 (2011).
- Shehnaz Ahmed, "Rise of Decentralised Finance | Reimagining Financial Regulation", 18 Indian Journal of Law and Technology 12 (2022).

Websites:

- Account Aggregator Framework, available at: https://financialservices.gov.in/beta/en/account-aggregator-framework (last visited on October 28, 2025).
- Akash Podishetti, "RBI Finally Lifts All Curbs on HDFC Bank, Including New Digital Launches", available at: https://www.livemint.com/industry/banking/rbi-finally-lifts-curbs-on-new-digital-launches-of-hdfc-bank-11647076803820.html (last visited on October 23, 2025).
- Ayush Chowdhury, Yash Jain, "Analysis of RBI Co-Lending Arrangements Directions, 2025", available at: https://corporate.cyrilamarchandblogs.com/2025/09/analysis-of-rbi-co-lending-arrangements-directions-2025/ (last visited on October 26, 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).
- Card Not Present Transactions - Relaxation In Additional Factor Of Authentication For Payments Upto

₹2000/- For Card Network Provided Authentication Solutions, available at: https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=2067 (last visited on October 25, 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).
- Constitutionality Of Aadhaar: Justice K. S. Puttaswamy (Union Of India) - Judgment In Plain English, available at: https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/ (last visited on October 29, 2025).
- Device Based Tokenisation - Card Transactions, available at: https://www.rbi.org.in/commonman/English/Scripts/FAQs.aspx?Id=2917 (last visited on October 25, 2025).
- Digital Lending Guidelines, available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3413 (last visited on October 23, 2025).
- Establishment of Digital Banking Units (DBUs), available at: https://ficci.in/public/storage/sector/Report/22068/RBI_DBU.PDF (last visited on October 30, 2025).
- FAQs On Master Direction On KYC, available at: https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=3782 (last visited on October 22, 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).
- Guidance Note On Operational Risk Management And Operational Resilience, available at: https://www.fidcindia.org.in/wp-content/uploads/2019/06/RBI-PRESS-RELEASE-OPERATIONAL-RISK-MANAGEMENT-30-04-24.pdf (last visited on October 28, 2025).
- Guidance Note On Operational Risk Management And Operational Resilience, available at: https://www.pdicai.org/Docs/RBI-2024-25-31_15202415340467.pdf (last visited on October 29, 2025).
- Guidelines on Default Loss Guarantee in Digital Lending, available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=3592 (last visited on October 28, 2025).
- India Cenbank Issues Guidance Note On Operational Risk Management And Resilience, available at: https://www.reuters.com/world/india/india-cenbank-issues-guidance-note-operational-risk-management-resilience-2024-04-30/ (last visited on October 29, 2025).
- Justice K. S. Puttaswamy (Retd.) And Anr. Vs Union Of India And Ors., available at: https://indiankanoon.org/

doc/91938676/ (last visited on October 24, 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 Information Technology Governance, Risk, Controls and Assurance Practices, available at: https://fidcindia.org.in/wp-content/uploads/2023/11/RBI-IT-MASTER-DIRECTIONS-07-11-23.pdf (last visited on October 24, 2025).
- Master Direction On Outsourcing Of Information Technology Services, available at: https://fidcindia.org.in/wp-content/uploads/2023/04/RBI-OUTSOURCING-OF-IT-SERVICES-10-04-23.pdf (last visited on October 25, 2025).
- Master Direction On Outsourcing Of Information Technology Services, available at: https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12486 (last visited on October 27, 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).
- Master Direction On Regulation Of Payment Aggregator (PA), available at: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896 (last visited on October 31, 2025).
- Online Dispute Resolution (ODR) System For Digital Payments, available at: https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=3194 (last visited on October 26, 2025).
- Payment And Settlement Systems - Storage Of Payment System Data (FAQs), available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995 (last visited on October 28, 2025).
- Ram Prakash Chaubey, "Cybercrime Investigation in India: An Analysis of Digital Evidence and Its Role in Proving Cybercrimes", available at: https://www.lawjournals.net/assets/archives/2025/vol7issue3/7067.pdf (last visited on October 31, 2025).
- RBI Cracks Down On Kotak Mahindra Bank; Bars Onboarding New Customers Through Online, Mobile Banking And Issuing New Credit Cards, available at: https://www.moneycontrol.com/news/business/rbi-bars-kotak-mahindra-bank-from-onboarding-new-customers-through-online-mobile-banking-issue-new-credit-cards-12707215.html (last visited on October 23, 2025).
- RBI Guidance on Loading of PPIs Through Credit Lines, available at: https://www.cyrilshroff.com/wp-content/uploads/2022/08/Insight-Newsletter.pdf (last visited on October 27, 2025).
- RBI Guidelines On Default Loss Guarantee (DLG) In Digital Lending, available at: https://ibclaw.in/rbi-

guidelines-on-default-loss-guarantee-dlg-in-digital-lending-dated-08-06-2023/ (last visited on October 26, 2025).

- RBI Lifts All Restrictions On HDFC Bank's New Digital Launches, available at: https://mas360.moneylife.in/article/rbi-lifts-all-restrictions-on-hdfc-bank-s-new-digital-launches/3989.html (last visited on October 24, 2025).
- RBI Simplifies KYC Rules To Allow Face-To-Face, Video And OTP-Based Onboarding For Customers, available at: https://economictimes.indiatimes.com/news/economy/policy/rbi-know-your-customer-kyc-rules-customer-onboarding-aadhaar-biometric-norms/articleshow/121797850.cms (last visited on October 31, 2025).
- RBI Tightens Default Loss Guarantee Rule; NBFCs To Exclude Cover On Fintech-Sourced Loans, available at: https://economictimes.indiatimes.com/industry/banking/finance/rbi-tightens-default-loss-guarantee-rule-nbfcs-to-exclude-cover-on-fintech-sourced-loans/articleshow/121420936.cms (last visited on October 25, 2025).
- Reconciling The Account Aggregator And Consent Manager Frameworks, available at: https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/ (last visited on October 31, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, available at: https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 30, 2025).
- The Bharatiya Nyaya (Second) Sanhita, 2023, available at: https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/173_2023_LS_Eng1212202342949PM.pdf?source=legislation (last visited on October 29, 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 Bharatiya Sakshya Adhiniyam, 2023 (No. 47 Of 2023), available at: https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.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 Reserve Bank - Integrated Ombudsman Scheme, 2021, available at: https://www.rbi.org.in/CommonPerson/english/Scripts/PressReleases.aspx?Id=3340 (last visited on October 30, 2025).
- Vijay Madanlal Choudhary And Ors. Vs Union Of India, available at: https://indiankanoon.org/doc/14485072/ (last visited on October 23, 2025).