ECA

Equi Corp Associates
Advocates & Solicitors

TRANSACTION • ADVISORY • LITIGATION

EQUICORP ASSOCIATES LLP

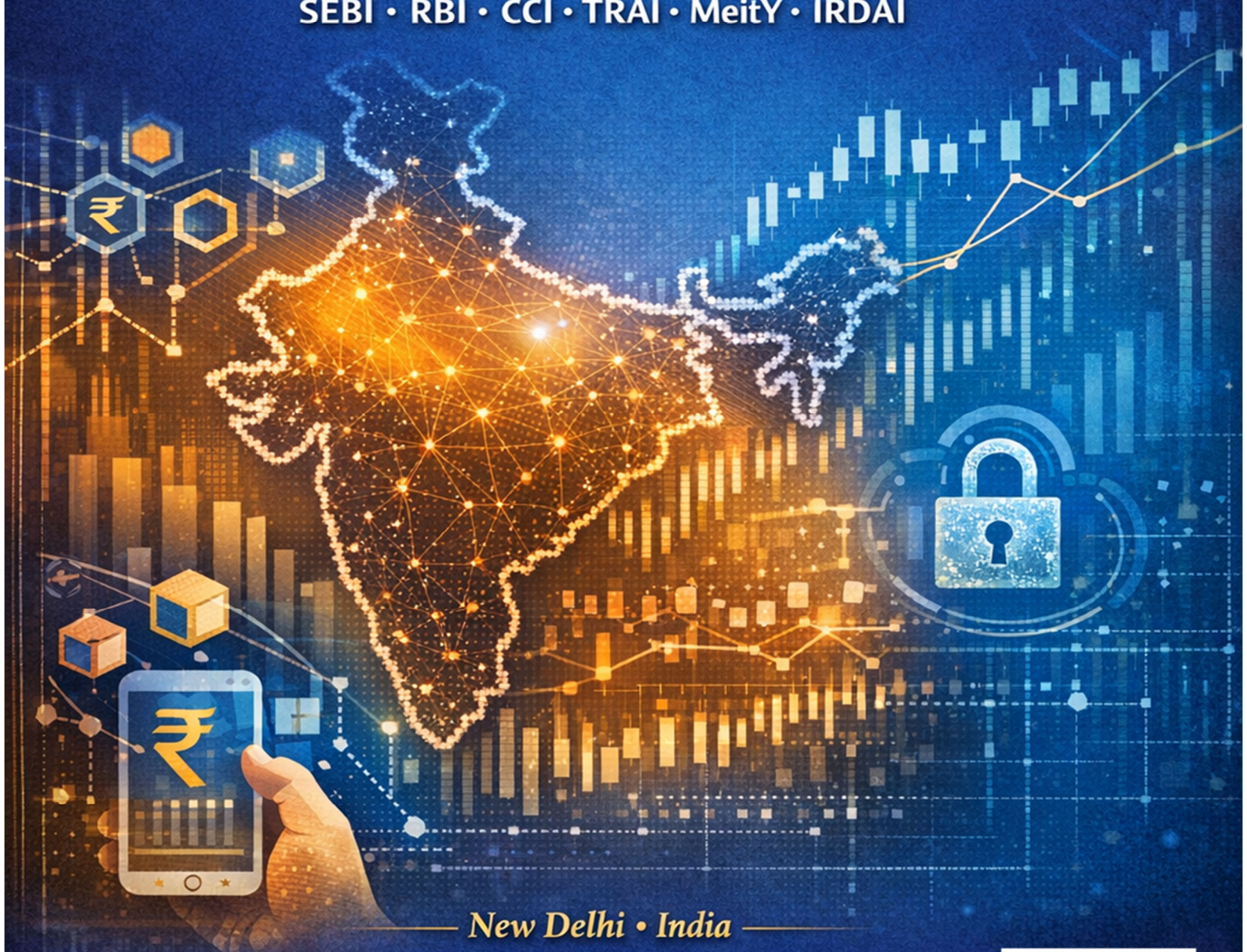
Advocates & Solicitors

LEGAL FRAMEWORK FOR DOING

FINTECH BUSINESS IN INDIA

A Professional Compendium on Regulatory Compliance

SEBI • RBI • CCI • TRAI • MeitY • IRDAI



New Delhi • India

C-98, 2nd Floor, East of Kailash, New Delhi – 110065, India

www.equicorplegal.com · admin@equicorplegal.com

TABLE OF CONTENTS

TABLE OF CONTENTS 1
PREFACE 4
CHAPTER I The Architecture of FinTech Regulation in India 5
1.1 Definitional Contours of "FinTech" 5
1.2 The Multi-Regulator Architecture 5
1.3 Constitutional and Legislative Foundations 7
1.4 Coordination Mechanisms 7
CHAPTER II Reserve Bank of India: Regulatory Framework 8
2.1 Payments and Settlement Infrastructure 8
2.1.1 Payment Aggregators and Gateways 8
2.1.2 Prepaid Payment Instruments 9
2.2 Non-Banking Financial Companies in the FinTech Space 9
2.2.1 NBFC-P2P Lending 9
2.2.2 Account Aggregators 10
2.3 Digital Lending Guidelines, 2022 10
2.4 Know Your Customer and AML Framework 12
2.5 RBI Regulatory Sandbox 12
CHAPTER III Securities and Exchange Board of India: FinTech Regulatory Regime 14
3.1 Registration Requirements for WealthTech Platforms 14
3.2 Alternative Investment Funds 14
3.3 Algorithmic Trading and High-Frequency Trading 15
3.4 SEBI's FinTech Regulatory Sandbox 15
CHAPTER IV Competition Commission of India: FinTech Market Regulation 18
4.1 The CCI's Market Study on FinTech (2021) 18
4.2 Horizontal and Vertical Restraints 18
4.3 Merger Control and FinTech Acquisitions 19
4.4 The Big Tech and Super-App Problem 20
CHAPTER V Telecom Regulatory Authority of India: FinTech Dimensions 21
5.1 TRAI's Regulatory Mandate and FinTech Intersections 21
5.2 DLT Platform for Commercial Communications 21
5.3 Over-the-Top Communication Services 22
5.4 Telecom and Financial Inclusion 23
CHAPTER VI Data Protection, Cybersecurity, and Digital Infrastructure 24
6.1 The Digital Personal Data Protection Act, 2023 24
6.2 CERT-In Directions, 2022 26
6.3 RBI Cybersecurity Framework 27

6.4 Cloud Computing Regulatory Framework 27
CHAPTER VII Master Regulatory Compliance Matrix 29
7.1 Payment Services Compliance Matrix....29
7.2 Digital Lending Compliance Matrix....30
7.3 WealthTech and Investment Platform Compliance Matrix 32
7.4 InsurTech Compliance Matrix....33
7.5 Data and Cybersecurity Compliance Matrix (Cross-Sectoral) 34
CHAPTER VIII Anti-Money Laundering and Counter-Financing of Terrorism....36
8.1 PMLA Framework and FinTech Obligations....36
8.2 FIU-IND Reporting Obligations....36
CHAPTER IX Open Finance, Account Aggregation, and Digital Public Infrastructure 38
9.1 The Account Aggregator Ecosystem....38
9.2 Compliance Architecture for NBFC-AAs 38
9.3 India Stack and Open Credit Enablement Network (OCEN) 39
CHAPTER X Enforcement, Penalties, and Regulatory Dispute Resolution....40
10.1 RBI Enforcement Mechanisms....40
10.2 SEBI Enforcement Mechanisms....40
10.3 CCI Enforcement Mechanisms....41
10.4 Regulatory Sandbox — Enforcement Implications....41
CHAPTER XI Concluding Observations and Emerging Issues....42
11.1 Regulatory Convergence and the Case for a Unified FinTech Statute....42
11.2 Emerging Regulatory Issues....42
11.3 Recommended Compliance Infrastructure 43
DISCLAIMER....45

PREFACE

The Indian financial technology sector has, in less than a decade, transformed from a peripheral adjunct to formal financial services into one of the primary engines of credit intermediation, payment settlement, insurance distribution, and capital formation in the country. India's Unified Payments Interface now processes transactions aggregating to values exceeding the nominal GDP of several medium-sized economies; account aggregators are reshaping the architecture of consent-based data sharing; digital lending platforms have extended credit to segments previously unserved by scheduled commercial banks; and robo-advisory services are democratising investment management.

Yet this dynamism unfolds against a regulatory landscape of remarkable complexity. Unlike certain jurisdictions where a single omnibus FinTech statute governs the sector, India's regulatory framework is the product of layered, often overlapping mandates exercised by at least six major regulators — the Reserve Bank of India, the Securities and Exchange Board of India, the Competition Commission of India, the Telecom Regulatory Authority of India, the Insurance Regulatory and Development Authority of India, and the Ministry of Electronics and Information Technology — each operating under distinct parent legislation and pursuing, not always harmoniously, distinct regulatory objectives.

This compendium is written for the practising advocate, in-house counsel, compliance officer, CEO, CFO, CTO and informed executive who must navigate this terrain with precision. It synthesises the primary regulatory instruments, presents detailed compliance matrices for each regulatory domain, analyses enforcement trends, and examines the emerging architecture of open finance and digital public infrastructure.

EquiCorp Associates LLP

New Delhi, June 2026

CHAPTER I
The Architecture of FinTech Regulation in India

1.1 Definitional Contours of "FinTech"

The term "financial technology" or "FinTech" lacks a statutory definition in Indian law. Regulators have employed varied descriptors: the Reserve Bank of India's Regulatory Sandbox Directions, 2019 refer to "innovative FinTech products, services or technology", while the SEBI Circular of 2021 speaks of "use of technology to solve problems in financial services." For the purpose of this compendium, FinTech encompasses any commercially operated platform, application, or infrastructure that deploys technology — including artificial intelligence, distributed ledger technology, application programming interfaces, and cloud computing — to facilitate, intermediate, or disrupt the delivery of financial services regulated under Indian law.

The sector may be broadly segmented into eight verticals: **(i) Payment Systems and Wallets; (ii) Digital Lending; (iii) WealthTech and Robo-Advisory; (iv) InsurTech; (v) RegTech and Compliance Automation; (vi) Account Aggregation and Open Banking; (vii) Crypto-Assets and Distributed Ledger; and (viii) Digital Neo-Banking**. Each vertical attracts a distinct regulatory schema, though overlapping licences and dual-regulator oversight are common.

1.2 The Multi-Regulator Architecture

India's financial regulatory architecture is structurally sectorised rather than unified. The principal regulators and their foundational statutes are as follows:[1]

Regulator	Parent Statute	Primary FinTech Mandate	Key Instrument(s)
Reserve Bank of India (RBI)	RBI Act, 1934; Banking Regulation	Payment systems, digital lending, NBFC-P2P,	Master Directions; Circulars; Regulatory

[1]Reserve Bank of India Act, 1934 (2 of 1934), as amended by the Reserve Bank of India (Amendment) Act, 2006 (26 of 2006), s. 45-IA (licensing of NBFCs).

Regulator	Parent Statute	Primary FinTech Mandate	Key Instrument(s)
	Act, 1949; PSS Act, 2007	account aggregators, forex	Sandbox Directions, 2019
SEBI	SEBI Act, 1992; SCRA, 1956; Depositories Act, 1996	WealthTech, robo-advisory, algo-trading platforms, AIF, digital broking	IA Regulations; PMS Regulations; AIF Regulations; FinTech Sandbox Circular 2021
Competition Commission of India (CCI)	Competition Act, 2002	Market dominance, anti-competitive agreements, merger control in FinTech	FinTech Market Study 2021; Combination Regulations
TRAI	TRAI Act, 1997; IT Act, 2000 (overlap)	OTT communication, SMS/USSD channels, DLT blockchain for SMS, telemarketing	TCCCPR, 2018; OTT Recommendations, 2020
IRDAI	Insurance Act, 1938; IRDAI Act, 1999	InsurTech, e-commerce of insurance, digital insurance intermediaries	E-Commerce Guidelines, 2017; Sandbox Guidelines, 2019
MeitY / Data Protection Board	IT Act, 2000; DPDP Act, 2023	Data protection, cybersecurity, intermediary	SPDI Rules, 2011; DPDP Act, 2023; CERT-In Directions, 2022

Regulator	Parent Statute	Primary FinTech Mandate	Key Instrument(s)
		liability, encryption policy	

1.3 Constitutional and Legislative Foundations

The constitutional basis for financial regulation in India rests principally on Entry 45 (banking) and Entry 46 (bills of exchange, cheques) of List I (Union List), Seventh Schedule. Payment systems regulation draws on Entry 45 read with the sovereign's currency management prerogative. The Information Technology Act, 2000 (IT Act) provides the overarching framework for electronic records and digital signatures, while the Prevention of Money Laundering Act, 2002 (PMLA) and the Foreign Exchange Management Act, 1999 (FEMA) impose horizontal obligations that cut across all FinTech verticals.[2]

The absence of a unified FinTech statute has engendered regulatory arbitrage, particularly at the boundary between payment facilitation (RBI jurisdiction) and securities settlement (SEBI jurisdiction), and between digital lending (RBI) and insurance premium financing (IRDAI/RBI). Courts have, on multiple occasions, been called upon to resolve jurisdictional ambiguity, though the tendency of the Supreme Court and High Courts has been to uphold concurrent regulatory authority rather than to delimit exclusive spheres.

1.4 Coordination Mechanisms

The Financial Stability and Development Council (FSDC), established in 2010 by executive order and chaired by the Finance Minister, serves as the apex inter-regulatory body. The FSDC Sub-Committee, chaired by the RBI Governor, provides operational coordination. A dedicated FinTech Department was established within the RBI in January 2022, reflecting the regulator's intent to consolidate its approach to technology-driven financial services. The Inter-Regulatory Technical Group on FinTech under the FSDC framework provides the forum for resolution of jurisdictional disputes and issuance of harmonised guidance.

[2]Payment and Settlement Systems Act, 2007 (51 of 2007), s. 7 (authorisation of payment systems).

CHAPTER II
Reserve Bank of India: Regulatory Framework

2.1 Payments and Settlement Infrastructure

The Payment and Settlement Systems Act, 2007 (PSS Act) provides the primary legislative basis for the RBI's oversight of payment systems. Section 7 of the PSS Act mandates that no person shall commence or operate a payment system without authorisation from the RBI, the grant of which is discretionary and conditioned upon compliance with systemic risk, operational resilience, and consumer protection requirements.[3]

The regulatory architecture for payments comprises three principal layers: (i) the system operator layer (National Payments Corporation of India for retail payments; CCIL for financial market settlement); (ii) the intermediary layer (Payment Aggregators, Payment Gateways); and (iii) the instrument layer (Prepaid Payment Instruments, UPI apps, mobile banking). Each layer is governed by specific Master Directions or Circulars.

2.1.1 Payment Aggregators and Gateways

The RBI's Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020 introduced a mandatory authorisation regime for payment aggregators (PAs) — entities that facilitate e-commerce transactions by accepting payments from customers on behalf of merchants and settling the same. Payment gateways (PGs), which provide only the technical infrastructure, are not required to seek RBI authorisation but must comply with specified security standards.[4]

Key Compliance Obligations: Payment Aggregators (RBI, 2020)

• Net worth: Minimum ₹15 crore at the time of application, to be increased to ₹25 crore by March 31, 2023.

[4]Reserve Bank of India, Guidelines on Regulation of Payment Aggregators and Payment Gateways, RBI/2019-20/188 DPSS.CO.PD.No.1810/02.14.008/2019-20 (Mar. 17, 2020).

• Nodal/Escrow Account: Mandatory maintenance with a scheduled commercial bank; funds to be settled within T+1 business day.

• Merchant onboarding: Mandatory background checks and KYC verification of merchants in line with the PA KYC Guidelines.

• Data Storage: Prohibition on storage of card data; adherence to PCI-DSS standards mandated.

• System audit: Annual security audit by CERT-In empanelled auditors; submission of audit reports to RBI.

• Grievance Redressal: Appointment of Nodal Officer; integration with RBI's Ombudsman Scheme for Digital Transactions.

2.1.2 Prepaid Payment Instruments

The Master Direction on PPIs, 2021 governs the issuance of closed-system, semi-closed, and open-system PPIs. Full-KYC PPIs may be issued up to a maximum balance of ₹2,00,000, while minimum-detail PPIs (now being phased into full-KYC within 24 months) are capped at ₹10,000. Interoperability between PPIs via UPI has been mandated for full-KYC PPIs.[5]

2.2 Non-Banking Financial Companies in the FinTech Space

The NBFC framework under Sections 45-IA to 45-MB of the RBI Act, 1934 has been extended to cover several FinTech-specific categories. The principal FinTech-relevant NBFC categories are: NBFC-Peer to Peer Lending Platform (NBFC-P2P); NBFC-Account Aggregator (NBFC-AA); and digital lending platforms operating as loan service providers (LSPs) in association with regulated entities.[6]

2.2.1 NBFC-P2P Lending

[5]Reserve Bank of India, Master Direction – Prepaid Payment Instruments (PPIs) (Updated as on Aug. 27, 2021), RBI/DPSS/2021-22/89.

The Master Directions on NBFC-P2P, 2017 establish a dedicated licence category for platforms that facilitate peer-to-peer lending by matching lenders and borrowers. The aggregate exposure of a lender across all P2P platforms is capped at ₹50,00,000; the exposure to a single borrower across all P2P platforms is capped at ₹10,00,000; and the maturity of loans must not exceed 36 months. Platforms may not lend from their own books and must maintain funds in an escrow account managed by a SEBI-registered trustee.[7]

The NBFC-P2P Directions were substantially amended in August 2024 following a series of RBI observations regarding cross-selling of credit enhancement products and off-balance-sheet exposure risks. Platforms are now prohibited from providing any form of credit guarantee, first loss default guarantee in excess of prescribed thresholds, or liquidity facility to lenders.

2.2.2 Account Aggregators

The NBFC-Account Aggregator (NBFC-AA) Directions, 2016 (amended 2021) govern entities that consolidate financial information held by regulated entities (Financial Information Providers or FIPs) and transmit it, with explicit, revocable, and granular consent of the data principal, to authorised Financial Information Users (FIUs). The AA framework is the cornerstone of India's Open Finance architecture and operates over the Sahamati network infrastructure.[8]

An NBFC-AA must obtain a Certificate of Registration from the RBI and is prohibited from storing the financial data it transmits. The AA's sole business activity is consent management and data routing; it may not carry on any other financial business.

2.3 Digital Lending Guidelines, 2022

The RBI's Guidelines on Digital Lending, 2022, operationalising the recommendations of the Working Group on Digital Lending (November 2021), introduced a comprehensive framework addressing structural risks in the digital lending ecosystem — including disguised co-lending

[7]Reserve Bank of India, Master Direction – Non-Banking Financial Company – Peer to Peer Lending Platform (Reserve Bank) Directions, 2017, RBI/DNBR/2017-18/57 (Oct. 4, 2017).
[8]Reserve Bank of India, Account Aggregator Framework: Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016, RBI/DNBR/2016-17/45 (as updated 2021).

arrangements, data privacy violations by lending apps, and circumvention of usury norms through fee structures.[9]

Requirement	Applicable Entity	Regulatory Basis	Consequence of Non-Compliance
Loan disbursement/repayment only through regulated entity's bank account (no pass-through through LSP)	Regulated Entities + LSPs	RBI Digital Lending Guidelines 2022, para 5	Cancellation of co-lending arrangement; enforcement action against RE
Key Fact Statement (KFS) mandatory before loan execution	All digital lenders	RBI Digital Lending Guidelines 2022, para 9	Loan agreement may be voidable; consumer complaint before Ombudsman
Annual Percentage Rate (APR) disclosure including all fees	All digital lenders	RBI Digital Lending Guidelines 2022, para 10	Monetary penalty; reputational action
Prohibition on automatic increase in credit limit without explicit consent	Digital lending apps	RBI Digital Lending Guidelines 2022, para 12	Regulatory scrutiny; consumer action
Mandatory cooling-off period for loan prepayment (3–7 days)	RE and LSPs	RBI Digital Lending Guidelines 2022, para 11	Consumer can repay without prepayment charges

[9]Reserve Bank of India, Report of the Working Group on Digital Lending Including Lending Through Online Platforms and Mobile Apps, November 2021; operationalised by RBI, Guidelines on Digital Lending, RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 (Sept. 2, 2022).

Requirement	Applicable Entity	Regulatory Basis	Consequence of Non-Compliance
Data collection restricted to need-based; no access to phone contacts/gallery	Digital lending apps	RBI Digital Lending Guidelines 2022, para 8; DPDP Act 2023	App store delisting; MeitY enforcement; RBI direction to RE
Grievance officer designated by both RE and LSP	RE and LSP	RBI Digital Lending Guidelines 2022, para 15	Integration into RBI Ombudsman jurisdiction

2.4 Know Your Customer and AML Framework

The RBI's Master Direction on KYC, 2016 (updated 2024) establishes the due diligence framework applicable to all regulated entities. For FinTech entities operating as or in partnership with regulated entities, KYC compliance is non-negotiable and operates as a condition of licence continuance. The PMLA, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 complement the KYC framework by imposing reporting obligations to the Financial Intelligence Unit – India (FIU-IND).[10]

The introduction of Video-based Customer Identification Process (V-CIP) and the Aadhaar-based eKYC pathway (subject to UIDAI authentication) have significantly reduced the cost of onboarding for digital-first FinTech entities. However, regulated entities must ensure that biometric data processed through V-CIP meets the data minimisation standards under the DPDP Act, 2023 and is not retained beyond the prescribed period.[11]

2.5 RBI Regulatory Sandbox

[10]Reserve Bank of India, Master Direction on KYC, RBI/DBR/2015-16/18 (Feb. 25, 2016), updated periodically (last updated Mar. 2024).
[11]Ministry of Finance, Report of the Inter-Ministerial Committee for Finalisation of Amendments to PMLA and Complementary Legislations, 2019; see also Prevention of Money Laundering Act, 2002 (15 of 2003), s. 12 (maintenance of records).

The RBI's Regulatory Sandbox (Final) Directions, 2019 established a framework under which FinTech firms may test innovative products or services in a live environment with real consumers, subject to defined safeguards and regulatory relaxations. The sandbox operates in cohorts, each focused on a theme (e.g., retail payments, cross-border payments, MSME lending). Entities selected for the sandbox are exempt from certain provisions of applicable Master Directions during the testing phase, provided they obtain the RBI's written concurrence.[12]

[12]Reserve Bank of India, Regulatory Sandbox (Final) Directions, 2019, RBI/2019-20/170 DBOD.No.BD.BC.No.31/22.01.001/2019-20 (Aug. 13, 2019).

CHAPTER III
Securities and Exchange Board of India: FinTech Regulatory Regime

3.1 Registration Requirements for WealthTech Platforms

WealthTech platforms — digital interfaces that provide investment advice, portfolio management, or investment execution services — are required to register with SEBI under one or more of the following regulatory categories, depending on their precise business model:[13]

- Investment Adviser (IA): Regulated under SEBI (Investment Advisers) Regulations, 2013. Registration mandated for any entity providing investment advice for consideration, whether or not discretionary. The 2021 amendments significantly enhanced net-worth requirements (₹50 lakh for individuals; ₹150 lakh for non-individuals) and imposed a strict fee model (AUM-based or fixed fee; no trail commissions).
- Portfolio Manager (PM): Regulated under SEBI (Portfolio Managers) Regulations, 2020. Minimum investment per client: ₹50 lakh. Net worth requirement: ₹5 crore. Mandatory depository account in client's name.
- Research Analyst (RA): Regulated under SEBI (Research Analysts) Regulations, 2014. Any entity publishing investment research for compensation must register; this includes AI-generated research reports if commercially distributed.
- Stock Broker / Sub-Broker: Entities executing trades on behalf of clients must register as stock brokers or sub-brokers under SEBI (Stock Brokers) Regulations, 1992 and maintain membership of a recognised stock exchange.

3.2 Alternative Investment Funds

FinTech platforms that pool capital from sophisticated investors for deployment in start-ups, debt instruments, or real assets must register as Alternative Investment Funds (AIFs) under the SEBI (AIF) Regulations, 2012. AIFs are categorised into three classes: Category I (venture capital, SME

[13]Securities and Exchange Board of India Act, 1992 (15 of 1992), s. 12 (registration of intermediaries).

funds, social venture funds), Category II (debt funds, fund of funds), and Category III (hedge funds employing leverage and complex trading strategies). Minimum corpus: ₹20 crore; minimum investor commitment (other than manager): ₹1 crore.[14]

The introduction of the Limited Partnership framework under the Limited Liability Partnership Act, 2008 has facilitated the adoption of LP-GP structures for Category II and Category III AIFs, aligning Indian fund structures more closely with international norms. SEBI Circular No. SEBI/HO/AFD/SEC-1/P/CIR/2023/121 (July 2023) introduced Accredited Investor norms that enable higher leverage and customised fee structures for qualifying investors.

3.3 Algorithmic Trading and High-Frequency Trading

Algorithmic trading platforms are subject to SEBI's framework governing automated order execution, which includes mandatory exchange approval for each algorithm deployed, randomisation of order-to-trade ratios, kill-switch requirements, and quarterly review of algorithms. The SEBI Circular on Algorithmic Trading by Retail Investors (April 2022) regulates the proliferation of third-party algo providers who offer pre-packaged strategies to retail participants through broker APIs.

The critical compliance requirement under this framework is that the liability for the algo's compliance with the SEBI (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003 vests with the registered broker, not the third-party provider. This creates a contractual indemnification imperative in broker-API provider agreements.

3.4 SEBI's FinTech Regulatory Sandbox

SEBI's Framework for Regulatory Sandbox (2021) enables entities within the securities market ecosystem to test innovative products under a relaxed regulatory environment for up to 12 months. The sandbox is open to SEBI-registered intermediaries, recognised stock exchanges, depositories, and technology providers that are in a formal partnership with a registered intermediary.

[14] SEBI (Alternative Investment Funds) Regulations, 2012 (SEBI/LAD-NRO/GN/2012-13/04), reg. 3–10 (categories and registration).

Exemptions available within the sandbox include relaxations from certain provisions of the IA Regulations, AIF Regulations, and Intermediary Registration requirements.[15]

SEBI Registration Category	Threshold / Eligibility	Key Ongoing Obligations	Penalty for Violation
Investment Adviser (non-individual)	Net worth ₹150 lakh; NISM certification; 3-year experience	Suitability assessment; risk profiling; fee disclosure; no trail commission post-2021 amendment	Deregistration; penalty up to ₹1 crore (SEBI Act s. 15H)
Portfolio Manager	Net worth ₹5 crore; minimum investment ₹50 lakh per client; NISM Series-XXI-A	Monthly reporting to clients; disclosure of conflicts; prohibition on guaranteed returns	Deregistration; prosecution under SEBI Act s. 24; penalty up to ₹25 crore
Alternative Investment Fund (Cat. I/II)	Minimum corpus ₹20 crore; per-investor ₹1 crore (₹25 lakh for employees)	Annual audit; valuation policy; SEBI reporting; PPM compliance	Suspension; cancellation; prosecution
Research Analyst	Minimum qualification; NISM Series-XV; no conflict with broking	Disclosure of holdings; research independence; no front-running	Monetary penalty; deregistration
Stock Broker	Net worth requirements per exchange; SEBI + exchange registration	Client fund segregation; annual audit; cyber	Expulsion from exchange; penalty up to ₹25 crore; prosecution

[15]SEBI Circular No. SEBI/HO/IMD/DF2/CIR/P/2021/024 (Mar. 4, 2021) (regulatory sandbox framework for FinTech).

SEBI Registration Category	Threshold / Eligibility	Key Ongoing Obligations	Penalty for Violation
		resilience framework	

CHAPTER IV
Competition Commission of India: FinTech Market Regulation

4.1 The CCI's Market Study on FinTech (2021)

In January 2021, the CCI published its Market Study on the FinTech Sector in India — a landmark examination of competitive dynamics across payment systems, lending platforms, and investment services. The Study identified five structural competition concerns: (i) platform and data concentration; (ii) exclusionary conduct by large technology conglomerates; (iii) lock-in through interoperability restrictions; (iv) algorithmic pricing coordination; and (v) preferential self-referencing in super-app architectures.[16]

With respect to payment systems, the Study examined the oligopolistic structure of the UPI market, noting that two platforms — PhonePe and Google Pay — accounted for over 80% of transaction volumes. The Study considered whether market cap mechanisms (proposed at 30% of total UPI volumes per participant) constituted an appropriate regulatory instrument, ultimately recommending continued monitoring under the Competition Act, 2002 rather than immediate intervention.[17]

4.2 Horizontal and Vertical Restraints

Section 3 of the Competition Act, 2002 prohibits agreements between enterprises that cause or are likely to cause an appreciable adverse effect on competition (AAEC) within India. In the FinTech context, relevant horizontal restraints include: (i) price-fixing of MDR (Merchant Discount Rate) between payment aggregators; (ii) market allocation agreements between competing P2P platforms; and (iii) coordinated refusal to interoperate with rival wallets.[18]

[16]Competition Commission of India, Market Study on the FinTech Sector in India, January 2021 (hereinafter "CCI FinTech Study 2021").
[17]CCI FinTech Study 2021 (n 15) at 43–47 (examining UPI market concentration and network effects).
[18]Competition Act, 2002 (12 of 2003), ss. 3(1), 3(4) (anti-competitive agreements and vertical restraints).

Vertical restraints of concern in the FinTech sector include: (i) exclusive dealing arrangements between device manufacturers and pre-installed payment applications; (ii) tying of payment services to e-commerce marketplace participation; and (iii) most-favoured-nation (MFN) clauses in merchant agreements that prevent differential pricing across platforms. The CCI's investigation into MFN clauses in the context of e-commerce platforms (upheld in the National Company Law Appellate Tribunal) has direct implications for payment platforms that operate embedded within marketplaces.

4.3 Merger Control and FinTech Acquisitions

Sections 5 and 6 of the Competition Act, 2002 require compulsory notification to the CCI of combinations (mergers, acquisitions, and amalgamations) that meet specified asset or turnover thresholds. The thresholds were revised by the Competition (Amendment) Act, 2023 to introduce a deal value threshold, making acquisitions of data-rich FinTech start-ups with limited revenue but high strategic value potentially notifiable.[19]

The deal value threshold — acquisitions where the value of the transaction exceeds ₹2,000 crore and the target has substantial business operations in India — is of particular significance for FinTech M&A, given that acqui-hire transactions and data asset acquisitions rarely meet traditional turnover tests but can confer significant market power.

CCI Compliance Checklist: FinTech Enterprises

1. Pre-merger notification: Assess against revised combination thresholds (deal value ₹2,000 crore); file Form I or Form II with CCI within 30 calendar days of binding agreement.
2. Anti-competitive agreements: Review all merchant agreements, partnership contracts, and data-sharing arrangements for AAEC risk; particular scrutiny of MFN clauses and exclusivity arrangements.
3. Dominance assessment: If market share exceeds 40% in any relevant product/geographic market, assess all pricing and product decisions against the s. 4 abuse of dominance standard.

[19] Competition Act, 2002 (12 of 2003), ss. 5–6 (regulation of combinations).

4. Data access and interoperability: Ensure that data access refusals to competitors have objective justification; monitor developments under the Digital Markets regulatory proposals.

5. Algorithmic pricing: Implement audit trails for dynamic pricing algorithms to demonstrate absence of coordination with competitors.

4.4 The Big Tech and Super-App Problem

The CCI has, in suo motu proceedings, commenced examination of the conduct of large technology platform operators in the Indian payments and lending markets. The core concern is "ecosystem leveraging" — the use of dominance in a primary market (search, operating system, e-commerce marketplace) to foreclose competition in adjacent FinTech markets. The investigation into Google's conduct with respect to its Play Store policies and their application to UPI apps and digital lending apps represents the most significant CCI enforcement action in the FinTech sector to date.

CHAPTER V
Telecom Regulatory Authority of India: FinTech Dimensions

5.1 TRAI's Regulatory Mandate and FinTech Intersections

The Telecom Regulatory Authority of India Act, 1997 empowers TRAI to regulate telecommunications services, including the setting of tariffs, quality of service standards, and the protection of consumer interests. TRAI's relevance to FinTech arises principally in four contexts: (i) the regulation of Unstructured Supplementary Service Data (USSD) channels used for mobile banking; (ii) the distributed ledger technology (DLT) platform for commercial SMS through which OTPs and transactional messages are routed; (iii) the regulation of Over-the-Top (OTT) communication services; and (iv) telecom-linked financial inclusion initiatives.[20]

5.2 DLT Platform for Commercial Communications

The Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR) mandated the deployment of a DLT-based platform for the registration of commercial communicators, their message templates, and their access codes. For FinTech entities, compliance with the DLT framework is operationally critical: every OTP, transaction alert, promotional message, or service update sent through an SMS channel must be routed through a TRAI-registered telecom operator using a pre-approved message header (Sender ID) and template.[21]

TRAI / DLT Requirement	Applicable Entity	Compliance Action Required	Regulatory Consequence
Registration on DLT platform as Principal Entity	All businesses sending commercial SMS	Register entity on TSP/DLT platform; obtain unique PE-ID	SMS traffic blocked; delivery failure; FIU implications if OTP fails

[20] Telecom Regulatory Authority of India Act, 1997 (24 of 1997), s. 36 (power to make regulations).
[21] TRAI, Telecom Commercial Communications Customer Preference Regulations, 2018 (TRAI/7-1/2017-QoS(Vol.II)/pt.(1)/37).

TRAI / DLT Requirement	Applicable Entity	Compliance Action Required	Regulatory Consequence
Message header (Sender ID) registration	All commercial SMS senders	Register brand name as 6-character alpha header (e.g., HDFCBK)	Message delivery blocked by telecom operators
Message template pre-registration	All commercial SMS senders	Register each template type (transactional, service, promotional)	Template not matching registered pattern is blocked
Consent-based communication	Marketing/promotional SMS senders	Maintain customer consent records; respect DND preferences	Penalty up to ₹2 lakh per violation; TRAI direction to TSP to bar entity
Scrubbing of DND numbers	Promotional communicators	Clean marketing lists against National Customer Preference Register	Penalty; disconnection of bulk SMS access
USSD shortcode registration	Mobile banking / *99# service users	Coordinate with NPCI and TSPs for USSD channel access	Service outage; RBI escalation if mobile banking disrupted

5.3 Over-the-Top Communication Services

TRAI's Recommendations on Regulatory Framework for OTT Communication Services (2020) have significant implications for FinTech platforms that deploy in-app messaging, voice calls, or

video KYC using OTT communication channels. While the 2020 Recommendations stopped short of recommending a separate licensing regime for OTT communication providers, TRAI emphasised that OTT providers must comply with lawful interception requirements and that the issue of regulatory parity with licensed telecom operators remained live.[22]

For FinTech entities using OTT channels for transaction authentication (e.g., WhatsApp OTP, in-app voice banking), the principal regulatory risk arises from the potential future imposition of a licensed telecom operator (LTO) requirement, which could impose significant compliance costs. Entities should monitor TRAI's consultation processes and assess contingency communication architectures.

5.4 Telecom and Financial Inclusion

The *99# USSD (Unstructured Supplementary Service Data)-based mobile banking service, operated by NPCI in partnership with telecom operators, provides basic banking services (account balance, fund transfers, mini-statement) to feature phone users without internet connectivity. This service operates under a tripartite regulatory framework involving TRAI (for USSD channel charges), RBI (for payment system authorisation), and NPCI (for operational management). FinTech entities seeking to build on this infrastructure must enter into agreements with both NPCI and the relevant telecom operators.

[22]TRAI, Recommendations on Regulatory Framework for Over-the-Top Communication Services (Sept. 14, 2020).

CHAPTER VI
Data Protection, Cybersecurity, and Digital Infrastructure

6.1 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) received Presidential assent on August 11, 2023 and represents the most significant legislative development for the FinTech sector since the PSS Act, 2007. The DPDP Act establishes a rights-based data protection framework grounded in six core principles: purpose limitation, data minimisation, accuracy, storage limitation, reasonable security safeguards, and accountability. The Act does not employ a sectoral carve-out for financial data; accordingly, all personal data processing by FinTech entities — including credit data, transaction data, investment profiles, and insurance records — is regulated under its provisions.[23]

The DPDP Act distinguishes between Data Fiduciaries (entities that determine the purpose and means of processing) and Data Processors (entities that process on behalf of fiduciaries). FinTech entities will typically operate as Data Fiduciaries; their cloud service providers, analytics vendors, and KYC service providers will operate as Data Processors. The Act imposes primary liability on Data Fiduciaries and permits contractual pass-through to Processors.[24]

DPDP Act Obligation	Section Reference	Operational Implication for FinTech	Financial Penalty (Max)
Consent before processing personal data	Section 6	Redesign onboarding flows; granular consent per processing	₹250 crore

[23]Digital Personal Data Protection Act, 2023 (22 of 2023), s. 4 (grounds for processing personal data).
[24]Digital Personal Data Protection Act, 2023 (22 of 2023), ss. 5–6 (notice and consent requirements).

DPDP Act Obligation	Section Reference	Operational Implication for FinTech	Financial Penalty (Max)
		purpose; no dark patterns	
Notice to data principal	Section 5	Privacy notice in plain language; accessible before or at time of consent collection	₹200 crore
Accuracy of personal data	Section 8(3)	Reconciliation of credit data, KYC records, and investment profiles; grievance process for correction	₹50 crore
Security safeguards	Section 8(5)	Implement ISO 27001 / RBI IT Framework controls; access controls; encryption in transit and at rest	₹250 crore
Data breach notification	Section 8(6)	Notify Data Protection Board and affected persons "without delay"; draft	₹250 crore

DPDP Act Obligation	Section Reference	Operational Implication for FinTech	Financial Penalty (Max)
		Incident Response Plan	
Erasure / Right to be forgotten	Section 12	Implement data deletion on request (subject to retention mandates under PMLA, FEMA, IT Act)	₹50 crore
Significant Data Fiduciary obligations	Section 10	If designated as SDF: appoint Data Protection Officer (DPO), conduct Data Protection Impact Assessments (DPIA), appoint independent auditor	₹250 crore
Prohibition on children's data processing without parental consent	Section 9	Age verification at onboarding; parental consent mechanism for users under 18	₹200 crore

6.2 CERT-In Directions, 2022

The CERT-In Directions on Information Security Practices, Vulnerability and Cybersecurity Incidents (April 2022) impose sector-agnostic mandatory obligations on all entities operating in

India's cyberspace, including FinTech companies. The most operationally significant provisions are: (i) mandatory reporting of cybersecurity incidents to CERT-In within six hours of noticing the incident or being brought to notice; (ii) mandatory log retention for 180 days; and (iii) mandatory time synchronisation with the NIC traceable time source. Failure to comply constitutes an offence under the IT Act, 2000.[25]

The six-hour incident reporting window is exceptionally short by international standards (GDPR mandates 72 hours; the NIS2 Directive, 24 hours for initial notification). FinTech entities must establish automated incident detection and triage pipelines that can identify, classify, and initiate the CERT-In notification process within this compressed timeline.

6.3 RBI Cybersecurity Framework

The RBI's Master Direction on IT Governance, Risk, Controls and Assurance Practices (January 2024, superseding the earlier 2016 framework) establishes a detailed technology risk management framework applicable to all RBI-regulated entities. Key pillars include: IT Governance (Board-level oversight, IT Strategy Committee); Risk Management (IT Risk Assessment, Business Continuity Planning, Cyber Crisis Management Plan); Information and Cyber Security (Security Operations Centre, penetration testing, red team exercises); and IT Operations (change management, patch management, vendor risk management).[26]

6.4 Cloud Computing Regulatory Framework

The RBI's Draft Cloud Adoption Framework (December 2022) and subsequent guidance require regulated entities to ensure that cloud services used for financial data processing meet specific requirements: (i) data residency within India for critical data; (ii) right to audit and inspection for RBI; (iii) contractual provisions prohibiting cloud service providers from sub-contracting data processing without prior approval; and (iv) business continuity and disaster recovery arrangements that are independent of the primary cloud provider.[27]

[25]Information Technology Act, 2000 (21 of 2000), s. 43A read with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[26]Reserve Bank of India, Master Direction – Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023, RBI/2023-24/102 DoS.CO.CSITEG/SEC.10/31.01.015/2023-24 (Apr. 10, 2023).
[27]Reserve Bank of India, Draft Circular on Cloud Adoption Framework for Regulated Entities, Dec. 2022; see also RBI's Master Direction on IT Governance, Risk and Controls (2023).

SEBI's Circular on Cyber Security and Cyber Resilience Framework (2021) mandates that stock exchanges, clearing corporations, depositories, and qualified registered intermediaries maintain a Cyber Security and Cyber Resilience Policy (CSCRP) reviewed annually by the Board.[28]

[28]SEBI, Circular on Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporations and Depositories, SEBI/HO/MRD/DOP1G/CIR/P/2021/036 (Mar. 3, 2021).

CHAPTER VII
Master Regulatory Compliance Matrix

The following matrix synthesises the principal compliance obligations across all four primary regulators and MeitY, organised by business activity. The matrix is designed as a practical reference tool for FinTech compliance officers and counsel conducting regulatory gap analyses or preparing for regulatory inspections. It is current as of June 2026 and should be read alongside the detailed analysis in Chapters I through VI.

7.1 Payment Services Compliance Matrix

Obligation	Regulator	Instrument	Periodicity / Trigger
PSS Act Authorisation	RBI	PSS Act, s. 7; PSS Regulations, 2008	One-time (prior to commencement of operations)
Net worth maintenance (PA: ₹25 crore)	RBI	PA/PG Guidelines, 2020	Continuous; reported in annual financial statements
Escrow/Nodal account maintenance	RBI	PA/PG Guidelines, 2020, para 8	Continuous; daily settlement (T+1)
PCI-DSS compliance (PA)	RBI	PA/PG Guidelines, 2020, para 6.3	Annual recertification by QSA
Annual Security Audit (CERT-In empanelled)	RBI / MeitY	PA/PG Guidelines; CERT-In Directions 2022	Annual + on major system changes
Cyber incident reporting to CERT-In	MeitY/CERT-In	CERT-In Directions, 2022	Within 6 hours of detection

Obligation	Regulator	Instrument	Periodicity / Trigger
RBI Ombudsman integration (DPSS)	RBI	RBI Ombudsman Scheme, 2021	Continuous; quarterly reports on complaints
DLT registration for OTP/SMS	TRAI	TCCCPR, 2018	One-time; template updates as required
KYC/AML compliance (full-KYC PPI)	RBI	KYC Master Direction, 2016 (as amended)	Continuous; CDD refresh every 2/8/10 years (high/medium/low risk)
PMLA transaction reporting (STR/CTR)	FIU-IND	PMLA, s. 12; PML Rules, 2005	Within 7 days (STR); Monthly (CTR)
FEMA compliance (cross-border payments)	RBI/ED	FEMA, 1999; Master Direction on Exports/Imports	Continuous; periodic filings per Master Directions

7.2 Digital Lending Compliance Matrix

Obligation	Regulator	Instrument	Periodicity / Trigger
NBFC-P2P Certificate of Registration	RBI	NBFC-P2P Directions, 2017	One-time; renewal not required but changes require RBI approval
Escrow account with SEBI-registered trustee (P2P)	RBI	NBFC-P2P Directions, 2017, para 14	Continuous

Obligation	Regulator	Instrument	Periodicity / Trigger
KFS disclosure prior to loan disbursal	RBI	Digital Lending Guidelines, 2022, para 9	Every loan origination
APR disclosure (all-in cost)	RBI	Digital Lending Guidelines, 2022, para 10	Every loan origination and periodic statement
Cooling-off period (3–7 days)	RBI	Digital Lending Guidelines, 2022, para 11	Every loan origination
Prohibition on access to device contacts/gallery	RBI/MeitY	Digital Lending Guidelines, 2022, para 8; DPDP Act, 2023	Continuous; app store audit
LSP grievance officer designation	RBI	Digital Lending Guidelines, 2022, para 15	Continuous; contact details on website/app
PMLA reporting (lending threshold)	FIU-IND	PMLA, 2002; RBI KYC Direction	Per transaction trigger
Credit bureau reporting (CIBIL/Equifax/CRIF)	RBI	Credit Information Companies Regulation Act, 2005	Monthly (standard); within 15 days (default)
Fair Practices Code (NBFCs)	RBI	RBI Fair Practices Code	Continuous; annual Board review

Obligation	Regulator	Instrument	Periodicity / Trigger
		Circular, 2003 (as updated)	

7.3 WealthTech and Investment Platform Compliance Matrix

Obligation	Regulator	Instrument	Periodicity / Trigger
SEBI IA registration	SEBI	IA Regulations, 2013	One-time; annual fee; 3-year renewal
NISM certification of key personnel	SEBI	IA Regulations, 2013, Reg. 7; NISM Series X-A, X-B	Continuous; certification renewed every 3 years
Risk profiling of clients	SEBI	IA Regulations, 2013; SEBI Circular 2020	At onboarding; updated annually
Suitability assessment before advice	SEBI	IA Regulations, 2013, Reg. 16	Every advice interaction
Investment Advice Agreement execution	SEBI	IA Regulations, 2013, Reg. 19	Before first advice
Fee structure compliance (no trail commission)	SEBI	IA Amendment, 2020	Continuous; disclosures in client agreement
Conflicts of interest disclosure	SEBI	IA Regulations, 2013, Reg. 15	At onboarding; material updates immediately

Obligation	Regulator	Instrument	Periodicity / Trigger
AUM-based fee cap (2.5% per annum)	SEBI	IA Circular 2020	Continuous; quarterly review
Annual compliance audit	SEBI	IA Regulations, 2013, Reg. 19A	Annual; report to SEBI within 60 days
Cyber Security and Resilience (CSCRP)	SEBI	SEBI Cybersecurity Circular, 2021	Annual Board review; quarterly SOC monitoring

7.4 InsurTech Compliance Matrix

Obligation	Regulator	Instrument	Periodicity / Trigger
Insurance Broker/Web Aggregator registration	IRDAI	Insurance Brokers Regulations, 2018; IRDAI Web Aggregator Regulations, 2017	One-time; 3-year renewal
E-Insurance Account (eIA) compliance	IRDAI	IRDAI (Electronic Policy and E-Insurance Account) Guidelines, 2016	Continuous
Telematics data compliance (Motor InsurTech)	IRDAI / RBI	Motor Vehicles Act; IRDAI Motor Guidelines; DPDP Act	Continuous; DPIA required for telematics processing

Obligation	Regulator	Instrument	Periodicity / Trigger
Regulatory Sandbox (InsurTech)	IRDAI	IRDAI (Regulatory Sandbox) Regulations, 2019	Application-based; 6-month to 1-year cycle
Anti-money laundering (insurance)	FIU-IND	PMLA, 2002; IRDAI AML/CFT Guidelines	Continuous; Annual compliance programme update
Data localisation for insurance records	IRDAI / MeitY	IRDAI Guidelines on Data and Cybersecurity; DPDP Act	Continuous; servers in India for policyholders' data

7.5 Data and Cybersecurity Compliance Matrix (Cross-Sectoral)

Obligation	Regulator	Instrument	Periodicity / Trigger
Consent management architecture	Data Protection Board / MeitY	DPDP Act, 2023, ss. 5–6	Pre-onboarding; updated on change of purpose
Privacy Notice publication	Data Protection Board / MeitY	DPDP Act, 2023, s. 5	Continuous; updated within 30 days of change
Data breach notification (Board + data principals)	Data Protection Board	DPDP Act, 2023, s. 8(6)	Without delay (operationally: within 6 hours per CERT-In)

Obligation	Regulator	Instrument	Periodicity / Trigger
Appointment of DPO (if SDF)	Data Protection Board	DPDP Act, 2023, s. 10	Upon designation as SDF
DPIA for high-risk processing	Data Protection Board	DPDP Act, 2023, s. 10(2)(b)	Before commencing high-risk processing activity
Cyber incident reporting to CERT-In	MeitY / CERT-In	CERT-In Directions, April 2022	Within 6 hours of detection
Log retention (180 days)	MeitY / CERT-In	CERT-In Directions, April 2022	Continuous
Vulnerability Assessment and Penetration Testing (VAPT)	RBI / SEBI / IRDAI (sectoral)	RBI IT Framework; SEBI Cyber Circular	Annual (minimum); after major releases
SOC 2 / ISO 27001 certification	RBI (recommended); contractual norm	RBI IT Outsourcing Directions, 2023	Annual recertification
Cloud data residency (India)	RBI / IRDAI / MeitY	RBI Cloud Framework; IRDAI Data Guidelines	Continuous; vendor contract review

CHAPTER VIII
Anti-Money Laundering and Counter-Financing of Terrorism

8.1 PMLA Framework and FinTech Obligations

The Prevention of Money Laundering Act, 2002 (PMLA) imposes obligations on "Reporting Entities" — a category that includes banking companies, financial institutions, intermediaries registered under the SEBI Act, payment system operators, and any other entity notified by the Central Government. FinTech entities that operate as RBI-regulated payment aggregators, NBFC-P2Ps, NBFC-AAs, or SEBI-registered investment advisers fall squarely within the definition of Reporting Entity and are subject to the full suite of PMLA obligations.[29]

The core obligations under the PMLA for FinTech Reporting Entities are: (i) maintenance of records of all transactions including the audit trail; (ii) furnishing of information to FIU-IND through the statutory reporting framework; (iii) verification of the identity of clients and beneficial owners; and (iv) appointment of a designated Principal Officer for PMLA compliance.[30]

8.2 FIU-IND Reporting Obligations

FIU-IND reporting under the PML (Maintenance of Records) Rules, 2005 requires Reporting Entities to submit: (i) Cash Transaction Reports (CTRs) for cash transactions above ₹10,00,000 in a calendar month; (ii) Suspicious Transaction Reports (STRs) for any transaction, regardless of amount, that raises suspicion of money laundering or terrorist financing; (iii) Non-Profit Organisation Transaction Reports (NTRs); and (iv) Cross-Border Wire Transfer Reports (CCTRs) for international transfers above USD 25,000.

For digital payment platforms, the CTR obligation applies to aggregated wallet loads and transfers. STR obligations require platforms to implement transaction monitoring systems capable of detecting layering patterns, structuring, round-tripping, and anomalous transaction velocities.

[30]Financial Intelligence Unit – India, Guidelines for Reporting Entities under PMLA, FIU-IND/2023/06 (updated April 2023).

The FIU-IND's Guidelines for Reporting Entities (2023) provide a risk-based framework for designing transaction monitoring rules.

CHAPTER IX
Open Finance, Account Aggregation, and Digital Public Infrastructure

9.1 The Account Aggregator Ecosystem

The Account Aggregator framework, operationalised under the RBI's NBFC-AA Directions, represents the most significant structural innovation in India's financial data infrastructure since the introduction of UPI. The AA ecosystem comprises: Financial Information Providers (FIPs — banks, NBFCs, mutual funds, insurance companies, pension funds, depositories), Financial Information Users (FIUs — lenders, wealth managers, account aggregators themselves acting as FIUs for their customers), and Account Aggregators (licensed NBFC-AAs acting as consent brokers).[31]

The data flow under the AA framework is strictly consent-based and unidirectional: FIPs expose customer financial data through standardised APIs; the AA routes data from FIPs to FIUs pursuant to granular, time-bound, and revocable consents obtained from the data principal. Consent artefacts are digitally signed and verifiable. The AA is prohibited from accessing the substance of the data it routes.

9.2 Compliance Architecture for NBFC-AAs

Compliance Area	Requirement	Regulatory Basis	Notes
Licensing	Certificate of Registration from RBI as NBFC-AA; minimum net worth ₹2 crore	NBFC-AA Directions, 2016	Single-activity restriction; no other financial business

Compliance Area	Requirement	Regulatory Basis	Notes
Consent Management	Collect, store, and manage consent artefacts; revocation within 24 hours	NBFC-AA Directions, 2016; DPDP Act, 2023	Consent artefacts digitally signed; immutable audit trail
Data Prohibition	Absolute prohibition on storing, processing, or monetising financial data routed	NBFC-AA Directions, 2016, para 5	Technology architecture must be zero-knowledge at AA layer
API Standards	Adopt ReBIT technical specifications for AA ecosystem APIs	Sahamati/ReBIT API Framework	Quarterly API audit; compatibility testing with FIPs/FIUs
Grievance Redressal	Two-tier grievance mechanism; integration with RBI Ombudsman	NBFC-AA Directions; RBI Ombudsman Scheme	30-day resolution timeline
Cybersecurity	ISO 27001; VAPT; SOC monitoring; incident response within 6 hours	RBI IT Framework; CERT-In Directions	Annual third-party security audit

9.3 India Stack and Open Credit Enablement Network (OCEN)

The Open Credit Enablement Network (OCEN), developed under the auspices of iSpirt and operationalised through the Account Aggregator and GSTN infrastructure, enables lenders (Loan Service Providers participating in OCEN) to access standardised borrower financial data through AA consents and to originate loans on a cash-flow underwriting basis. OCEN's regulatory compliance obligations overlay the AA framework with additional KYC and lending regulations applicable to the participating NBFC or bank.

CHAPTER X

Enforcement, Penalties, and Regulatory Dispute Resolution

10.1 RBI Enforcement Mechanisms

The RBI's enforcement arsenal under the PSS Act, 2007 and the RBI Act, 1934 includes: (i) monetary penalties (under PSS Act, s. 30, up to ₹10 lakh per violation, each day of default counted separately; under Banking Regulation Act, s. 47A, up to ₹5 crore or twice the amount of the transaction); (ii) directions to cease and desist; (iii) cancellation of Certificate of Registration; (iv) appointment of an administrator; and (v) referral to enforcement agencies (ED, CBI) for PMLA and FEMA violations.[32]

The RBI established a dedicated Enforcement Department in 2017 to centralise enforcement actions and insulate supervisory functions from compliance functions. The Enforcement Department follows a structured escalation matrix: first, a show-cause notice specifying the alleged contravention; then, a personal hearing before the Enforcement Department; then, the issue of an order imposing penalty. Orders are appealable before the Central Government under the PSS Act and before the Writ Court on grounds of jurisdictional error or violation of natural justice.

10.2 SEBI Enforcement Mechanisms

SEBI's enforcement toolkit is among the most extensive of Indian financial regulators. Under Sections 11, 11B, and 11D of the SEBI Act, SEBI may issue directions, including directions to refund monies, cancel registration, and prohibit market access. Section 15H empowers SEBI to impose monetary penalties of up to ₹1 crore (for certain violations) or up to ₹25 crore (for certain specified violations including fraudulent/unfair trade practices). Section 24 makes certain violations punishable with imprisonment up to 10 years.[33]

[32]Reserve Bank of India, Framework for Imposing Monetary Penalty under the Payment and Settlement Systems Act, 2007; see PSS Act, s. 30 (penalties).
[33]Securities and Exchange Board of India Act, 1992 (15 of 1992), s. 15H (penalty for failure to comply with SEBI's directions).

SEBI's Securities Appellate Tribunal (SAT) is the designated appellate forum for challenges to SEBI orders. SAT decisions are appealable to the Supreme Court on questions of law. The time-limit for filing an appeal before SAT is 45 days from the date of the order (extendable on sufficient cause).

10.3 CCI Enforcement Mechanisms

The Competition Commission of India may impose penalties of up to 10% of the average turnover of the enterprise for the preceding three financial years for anti-competitive agreements (Section 27) and abuse of dominance (Section 4). For failure to notify a combination under Section 6, the penalty is up to 1% of total assets or turnover, whichever is higher, for the combination. For failure to comply with CCI's directions (Section 42), further penalties of ₹1 lakh per day apply.[34]

CCI orders are appealable before the National Company Law Appellate Tribunal (NCLAT) within 60 days of the order (extendable by 60 days on sufficient cause). NCLAT decisions are further appealable to the Supreme Court.

10.4 Regulatory Sandbox — Enforcement Implications

Entities operating within regulatory sandboxes (RBI, SEBI, IRDAI) enjoy limited but defined exemptions from specified provisions during the sandbox tenure. The regulatory exemption does not, however, extend to: (i) obligations under the PMLA, 2002; (ii) consumer protection requirements under the Consumer Protection Act, 2019; (iii) cybersecurity obligations under CERT-In Directions, 2022; or (iv) competition law. Sandbox participants should maintain a clear compliance register distinguishing exempted provisions from non-exempted ones, and should ensure that consumer disclosures accurately reflect the experimental nature of the product.

[34]Competition Act, 2002 (12 of 2003), s. 27 (penalties for anti-competitive practices), s. 43A (failure to notify combinations).

CHAPTER XI
Concluding Observations and Emerging Issues

11.1 Regulatory Convergence and the Case for a Unified FinTech Statute

The analysis in the preceding chapters reveals a regulatory landscape characterised by remarkable depth within individual domains but significant fragmentation at the boundaries. The RBI's transformation of the NBFC framework to accommodate P2P lending and account aggregation, SEBI's sandbox for WealthTech innovation, and TRAI's DLT platform for secure communications each represent thoughtful, domain-specific regulatory design. Yet the FinTech practitioner and the FinTech enterprise must simultaneously navigate these distinct regimes, comply with the overlapping obligations of the PMLA and DPDP Act, and manage the competition law dimension — all without the benefit of a unified compliance framework or a single supervisory authority.

The case for a unified FinTech statute — modelled on approaches adopted in Singapore (through the MAS's Payment Services Act, 2019) or the UK (through the FCA's integrated FinTech regulatory perimeter) — has been increasingly articulated in policy discourse. A consolidated statute would reduce compliance fragmentation, eliminate regulatory arbitrage, establish clear jurisdictional allocation, and provide a more predictable environment for FinTech investment. The RBI's FinTech Department and the FSDC Sub-Committee provide the institutional foundations for such harmonisation.

11.2 Emerging Regulatory Issues

Four regulatory developments merit close monitoring by FinTech practitioners in the near term:

- Artificial Intelligence in Financial Services: The Ministry of Finance's consultation on AI governance in financial services and RBI's guidance on the use of AI in credit underwriting remain at early stages. The intersection of AI explainability requirements and the DPDP Act's consent and accuracy obligations will require careful architectural planning, particularly for credit scoring models that rely on alternative data.

- Central Bank Digital Currency (CBDC): The RBI's retail and wholesale CBDC pilots, conducted under the Digital Rupee framework, introduce new regulatory questions regarding interoperability with the existing payment system, PMLA treatment of CBDC transactions, and the role of FinTech intermediaries in CBDC distribution.
- Digital Markets Regulation: The Competition (Amendment) Act, 2023 introduced a framework for systemic digital enterprises — potentially analogous to the European Digital Markets Act. The CCI is consulting on criteria for designation of Systemically Significant Digital Enterprises (SSDEs), which could impose ex ante interoperability, data-sharing, and self-preferencing obligations on large FinTech platforms.
- Crypto-Asset Regulation: India's current framework imposes a 30% tax on virtual digital asset (VDA) transfers (Finance Act, 2022) and 1% TDS on VDA transactions above prescribed thresholds, but lacks a comprehensive licensing or consumer protection framework for crypto-asset service providers. The pending Cryptocurrency and Regulation of Official Digital Currency Bill remains a source of significant regulatory uncertainty for Web3 FinTech enterprises.

11.3 Recommended Compliance Infrastructure

Given the complexity of the multi-regulator environment, FinTech enterprises operating across multiple verticals should establish the following governance infrastructure:

1. A Regulatory Compliance Committee at the Board level, with representation from at least one independent director with financial services regulatory experience.
2. A Chief Compliance Officer (CCO) with clearly defined authority, adequate resources, and a direct reporting line to the Board/Audit Committee, structurally independent of business functions.
3. A Regulatory Intelligence function responsible for tracking regulatory developments across RBI, SEBI, CCI, TRAI, IRDAI, MeitY, FIU-IND, and relevant Ministry notifications, and for updating the internal compliance register within 30 days of any regulatory change.
4. A single-source Compliance Register mapping each applicable regulation to the specific operational activity, responsible owner, compliance evidence, and periodic review date.

5. Annual external legal audit of the regulatory compliance programme, with a specific focus on emerging regulatory developments and areas of potential conflict between regulators.

— End of Compendium —

DISCLAIMER

This compendium has been prepared by EquiCorp Associates LLP for general informational purposes only. It does not constitute legal advice and is not a substitute for advice from qualified legal counsel in relation to any specific transaction, regulatory filing, or compliance question. The regulatory landscape for FinTech businesses in India is subject to frequent and material change; readers are advised to verify the current status of all instruments cited herein before acting on any information contained in this compendium. EquiCorp Associates LLP makes no representation as to the completeness or accuracy of this compendium and disclaims any liability for reliance on its contents.