Unified Fintech Forum
POWERING RESPONSIBLE FINTECH

KHAITAN &CO ADVOCATES SINCE 1911

Fintech Round-Up 2025 - 26

FOREWORD

The questions our members asked this year were different from the year before. Less "are we allowed to do this," and more "who is answerable if it goes wrong, and can we show how we decided." That change says a lot about the year we have just had.

The Reserve Bank chose to rebuild rather than patch. In November 2025, more than 9,000 circulars were turned into 238 Master Directions. The common thread is that the gaps between frameworks have closed. A lot of useful innovation used to sit in those gaps. So did a lot of avoidable harm. Firms that never held a licence now carry obligations — the offline aggregator, the AePS touchpoint operator, the lending service providers or the vendor whose model quietly prices someone's loan. If your product shapes a regulated entity's decision, you are inside the line.

The scrutiny has also changed in kind. Board-approved frameworks, single sources of truth, model inventories, testing records, explainability standards. Regulators now want to know how a decision was made, not only what the outcome was. There is real proportionality on offer in return — the three-tier NBFC classification and SEBI's lighter treatment of internal AI use are both sensible — but it has to be paid for in paperwork. That is a fair deal for firms that already work this way, and a hard one for firms that do not.

I will not pretend this lands evenly across our membership. A large fintech player (NBFC) can add a compliance function fairly quickly. A twenty-person team building on a bank's rails cannot do it at the same speed. UFF's job is to take that reality into the room — not to ask for weaker rules, but for practical timelines and clarity on who is responsible when four parties touch one transaction.

This Regulatory Round-Up Report would not exist without the team at Khaitan & Co. They read every direction, every draft and every consultation paper of the year, and then did the harder part: setting it out simply, with the background, the substance and the practical takeaway in one place. It is careful work, generously given, and our members are the better for it. My sincere thanks to them.

I am sure fintechs will use this report as a map, not as a substitute for advice on specific facts. The rules of this market are being written fast. Firms that read closely will find they have more room than they feared, and less time than they hoped. Once again, thanks to the authors of the report.

Jatinder Handoo

CEO

Unified Fintech Forum

FOREWORD

2025–26 has been a watershed year for India's financial regulatory landscape. Regulators have moved decisively from incremental, reactive interventions to constructing comprehensive, forward-looking frameworks that seek to balance the twin imperatives of fostering innovation and maintaining prudential discipline. This report, "Fintech Round-Up 2025–26", provides an in-depth analysis of the most significant regulatory milestones that have shaped the Fintech and financial services sector during this period.

At the centre of this transformation is the Reserve Bank of India's landmark consolidation exercise, which distilled over 9,000 regulatory circulars into 238 structured Master Directions—a foundational recasting of the regulatory canon. Alongside this, SEBI, IFSCA and other regulators have each advanced frameworks addressing the opportunities and risks presented by emerging technologies, digital assets and evolving market structures.

This report covers five key themes:

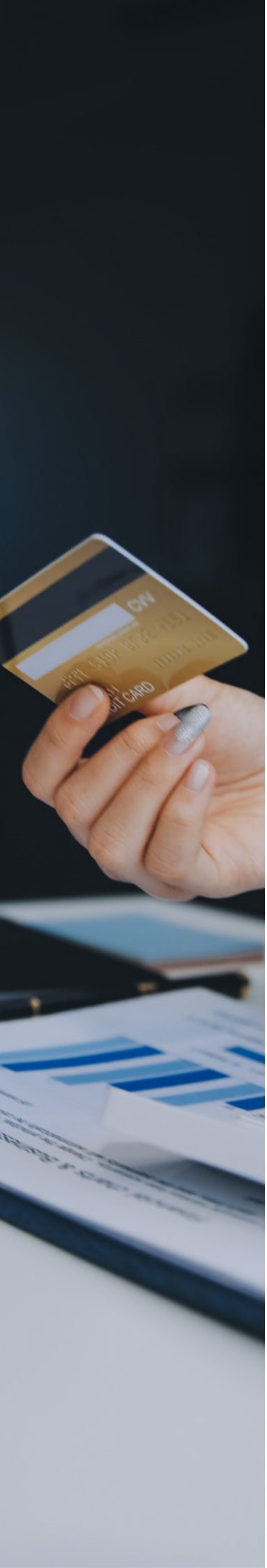
1. Lending, examining the RBI's unified related party lending framework, the opening of acquisition finance to banks, the recalibration of NBFC categorisation, and new conduct and distribution norms
2. Payments, analysing the unification of the payment aggregator regime across online, offline and cross-border channels, upgrades to authentication frameworks, and new AePS and prepaid payment instrument standards
3. Data Governance and Risk Management, covering the RBI's draft guidances on data governance and model risk management, with their far-reaching implications for AI/ML deployment
4. Securities and Investment Platforms, addressing SEBI's consultations on responsible AI usage, harmonised advertising standards, electronic trading platform reforms and the digital gold advisory
5. IFSCA, examining the regulatory approach to tokenisation of real-world assets and the consolidation of the TechFin and ancillary services framework in GIFT City.

We believe this report will serve as an essential resource for Fintech companies, financial institutions, investors, and stakeholders navigating India's evolving regulatory environment. As the sector matures, the collaboration between regulators, industry participants, and legal practitioners will remain critical in ensuring that innovation thrives within a framework of responsible governance and consumer protection.

We hope you find this a valuable reference as you chart your course through the regulatory developments of the year ahead.

Smita Jha
Partner
Khaitan & Co

Prashanth Ramdas
Partner
Khaitan & Co



Contents

01

LENDING

India's financial regulatory architecture has entered a new epoch. As credit markets deepen and diversify, the Reserve Bank of India has transcended the reactive, crisis-driven posture of earlier decades, embracing instead a systematic, anticipatory approach to supervision. The developments of 2025–26 bear the unmistakable imprint of this transition: a deliberate, institution-wide effort to construct coherent regulatory frameworks that accommodate the imperatives of growth while preserving the discipline essential to prudential stability.

At the heart of this transformation lies the RBI's landmark consolidation exercise of 28 November 2025—a singular administrative undertaking that distilled more than 9,000 extant regulatory circulars into 238 function-wise Master Directions, each tailored to distinct categories of regulated entities. The CRM Directions, SBR Directions, SCB Credit Directions, NOFHC Directions and the suite of NBFC-specific directions examined in this chapter emerge from that consolidation. What might appear as mere reorganisation is, in truth, a foundational recasting of the regulatory canon, replacing the palimpsest of incremental circulars with structured, navigable frameworks.

The sophistication of this new regulatory architecture is evident in the particulars. The CRM Amendment Directions introduce a harmonised framework governing lending to related parties across eight categories of regulated entities—closing longstanding supervisory lacunae with a single, coordinated intervention of remarkable breadth. The CME Amendment Directions open the gates of acquisition finance and leveraged buyouts to Indian banks, within a carefully calibrated prudential structure that balances ambition with caution. The Third SCB Credit Amendment Directions extend the reach of bank credit to REITs, subject to robust safeguards that reflect a measured embrace of new asset classes.

For NBFCs—whose assets under management have swelled to INR 57.88 trillion by FY 2026, reflecting a compound annual growth rate of 17.5% over two years—the governance framework has been refined with equal deliberation. The First and Second SBR Amendment Directions recalibrate the scale-based regulatory architecture, acknowledging a self-evident truth: that NBFCs neither availing public funds nor maintaining customer interface present a markedly attenuated systemic-risk profile. The resulting three-tier classification applies proportionate oversight calibrated to genuine risk, not notional uniformity. The NBFC Undertaking of Financial Services amendments consolidate fragmented, product-specific distribution regimes into a unified agent-principal structure, bringing clarity where opacity once prevailed.

The NOFHC Amendment exemplifies the same impulse towards regulatory efficiency: the erstwhile prior-approval regime for specified financial activities gives way to an intimation-based framework, reducing regulatory friction for banking groups whilst preserving the supervisory visibility essential to systemic oversight.

The pattern that emerges is unmistakable: the RBI is constructing a regulatory ecosystem suited to a larger, more complex, more interconnected financial system—one that prizes coherence over accumulation, proportionality over uniformity, and institutional governance over transactional approvals. This

is supervision for a maturing economy, and the lending reforms of 2025–26 stand as its clearest expression.

Set out below are the key regulatory developments in the lending space during 2025-26.

Keeping it in the Family: RBI's Unified Related Party Lending Framework

BACKGROUND

On 5 January 2026, RBI issued eight simultaneous CRM Amendment Directions, one for each category of RE (SCBs, SFBs, LABs, RRBs, UCBs, RCBs, NBFCs (including HFCs) and AIFIs), introducing a unified framework governing lending to related parties across all REs.

The CRM Amendment Directions took effect from 1 April 2026, with REs permitted to adopt them earlier.

ANALYSIS

Expanded Definitions and Scope:

Related Person: A 'Related Person' includes a person (and their relatives) who:

Is a promoter, director or KMP of the RE

Owns more than 5% of paid-up equity share capital or voting rights

Can nominate a director

Controls the RE. Carve-outs exist for director-nomination rights arising solely from lending arrangements, advice given in a professional capacity, and government-owned entities with common government ownership

Related Party: A 'Related Party' extends to related persons, a reciprocally related person or any entity where a related person holds a position of influence, including entities where they are a partner, director, promoter, hold more than 10% paid-up equity share capital or control more than 20% voting rights, exercise control or are a guarantor, trustee or beneficiary of a private trust.

Materiality Thresholds: Loans to related parties are subject to materiality thresholds calibrated to the size and category of each RE. Loans above the threshold must be sanctioned by the Board or a dedicated 'Committee on Lending to Related Parties' (a Board committee other than the ACB).

Regulatory Prohibitions and Exemptions: For SCBs and SFBs, the prohibition on lending to directors is extended to:

- Spouses and minor / dependent children of directors
- Promoters and their relatives
- In case of SCBs and SFBs, shareholders with shareholding of 10% or more in the paid-up equity capital of the respective SCB or SFB
- Their controlled entities

Recusal, Monitoring and Transitional Provisions: Directors, KMPs and specified employees must recuse themselves from deliberations on loan proposals or arrangements involving themselves or their related parties. REs must maintain and periodically update a register of all related persons and related parties, with quarterly reviews of adherence. Deviations must be reported to the ACB.

Enforcement: Non-compliance may attract monetary penalties, full provisioning requirements, forensic audits and other enforcement actions. Existing non-conforming facilities may run off until maturity but cannot be renewed, reviewed or enhanced.

Key Takeaways

The CRM Amendment Directions mark a step-change in RBI's oversight of related party lending. By establishing a unified framework across all RE categories, RBI seeks to close regulatory gaps that previously allowed related parties to operate outside the supervisory perimeter, while providing REs with predictable parameters (well-defined materiality thresholds, structured approval hierarchies and standardised monitoring obligations) within which related party transactions may proceed.

Reorganising the Regulatory Architecture For NOFHC-Held Entities

BACKGROUND

An NOFHC is an NBFC registered with RBI that does not itself carry on financial operations. It serves as a holding entity through which promoters of a group hold a banking company and all other regulated financial services entities, ring-fencing them from the group's commercial and unregulated activities.

Previously, specialised financial activities such as insurance, mutual funds and broking services had to be carried out through a separate subsidiary, JV or associate under the NOFHC, with prior RBI approval. The NOFHC Amendment, issued on 5 December 2025 and effective immediately, replaces this with an intimation-based framework.

ANALYSIS

Activities Permitted to a Bank: The NOFHC Amendment reiterates that all activities permitted to be undertaken by a bank under Section 6(1)(a) to (o) of the BR Act shall be carried out from the bank itself, reinforcing the principle of functional segregation between core banking operations and specialised financial activities of the group.

Specialised Activities: The NOFHC Amendment specifies that the following specialised activities shall be carried out only through subsidiary, JV or associate structures of a bank held by the NOFHC:

- Mutual fund business
- Insurance business
- Pension fund management
- Investment advisory and management services
- Portfolio management services
- Broking services

All other activities permitted under the BR Act may be carried out departmentally by a bank.

Shift from Prior Approval to Intimation: Significantly, an NOFHC no longer requires the prior approval of RBI for entities held by it to undertake the specialised activities listed above, unless advised otherwise by RBI. Instead, the NOFHC is required to intimate RBI within 15 days from the date of the board resolution authorising the undertaking of such businesses. This replaces the earlier requirement of prior RBI approval where promoters desired to continue or commence specialised activities from a separate entity held under the NOFHC.

Prior Approval Retained for Other Business: An NOFHC will continue to require the prior approval of RBI for entities held by it to undertake any other form of business, subject to other applicable instructions. The NOFHC Amendment also retains a group-level restriction that activities not permitted to be undertaken by a bank are not permitted by the entities held by the NOFHC.

Key Takeaways

The NOFHC Amendment materially reduces the regulatory lead time for groups seeking to commence mutual fund, insurance, pension fund management, investment advisory and management, portfolio management or broking services through NOFHC-held entities. By replacing prior approval with a 15-day post-Board-resolution intimation, RBI has streamlined group-level governance while preserving oversight over non-specified activities.

Banks at the Table: A New Era for Acquisition Finance

BACKGROUND

On 24 October 2025, RBI proposed greater financing flexibility for corporate acquisitions, higher limits on loans against shares and REIT / InvIT units, and removal of regulatory ceilings on lending against listed debt securities. Following stakeholder feedback, RBI issued a revised version on 30 March 2026 (CME Amendment Directions), effective 1 July 2026.

ANALYSIS

The CME Amendment Directions recalibrate the norms relating to acquisition finance, bridge finance, loans against securities and exposure to capital market intermediaries.

Acquisition finance defined: A financial facility for acquiring control over a target company (domestic or foreign), including through merger or amalgamation. Instruments include equity shares, CCPS and CCDs. Refinancing of target-company debt is permitted where integral to the acquisition. Standalone financing of fixed-asset purchases through slump sales falls outside the framework.

Eligible borrowers:

- An Indian non-financial company as acquirer
- An existing non-financial subsidiary (in India or overseas)
- A step-down SPV set up for the acquisition. InvITs acquiring equity or CCDs are also eligible. Financial entities (NBFCs, AIFs) are excluded

Acquirer criteria: Minimum net worth of INR 500 crore and net profit in each of the three preceding financial years. Unlisted acquirers must hold an investment-grade rating (BBB- or above).

Control acquisition: Control may be established through a single transaction or interconnected transactions completed within 12 months. Where the acquirer already holds control, acquisition finance may only be extended for crossing substantial thresholds of 26%, 51%, 75% or 90% voting rights.

Related party bar: Acquisition finance is barred where acquirer and target are related parties under the Companies Act, 2013 or under common control, management or promoter group, except for crossings of the substantial thresholds noted above.

Financing cap: Bank financing capped at 75% of acquisition value, with 25% from own funds (internal accruals, fresh equity or asset sales). Listed acquirers may use secured bridge finance for the own-funds contribution, repayable within 12 months.

Prudential requirements: Credit assessment on a pro-forma consolidated basis. Corporate guarantee mandatory where the facility is extended to a subsidiary or SPV. Post-acquisition debt-to-equity ratio at consolidated level must not exceed 3:1.

Security: Acquisition finance is stipulated to be secured by the financial instruments issued by the target company through which control over it is acquired; additional collateral (unencumbered assets, promoter guarantee) per bank policy may also be provided.

Exposure limits: Each bank's aggregate acquisition-finance exposure capped at 20% of eligible capital base, within the overall capital market exposure ceiling of 40%.

Loans against eligible securities: A new principle-based framework replaces the existing regime for loans against shares, debentures and bonds. "Eligible securities" now cover listed Group-1 equity shares, government securities, listed debt rated BBB or higher, mutual fund and ETF units, and REIT / InvIT units, with prescribed LTV ceilings for individuals.

Credit facilities to CMIs: A new chapter permits need-based, fully secured credit facilities for working capital, margin trading financing, settlement mismatches and market-making. Proprietary trading and investments by CMIs remain excluded, except for approved market makers and debt-warehousing (up to 45 days).

Key Takeaways

Transformative shift: Indian banks can now participate in leveraged buyouts and control acquisitions previously dominated by private credit funds, FPIs and NBFCs — creating a competitively priced domestic leverage option for corporates and sponsor-led transactions.

Structural safeguards: The framework balances flexibility with prudential discipline through financing caps, own-funds requirements, pro-forma credit assessment, mandatory guarantees, leverage ceilings and aggregate exposure limits.

Refinancing and bridge finance: Express recognition of target-company debt refinancing and availability of bridge finance for listed acquirers adds structural flexibility for complex transactions.

Implementation details: Several aspects — underwriting benchmarks, exposure limits, nature and extent of security cover — remain subject to individual bank policies, creating scope for divergent interpretation across lenders.

Change in Scales: NBFC Categorisation

BACKGROUND

RBI amended the SBR Directions by way of the First SBR Amendment Directions on 29 April 2026, effective 1 July 2026, followed by the Second SBR Amendment Directions on 24 June 2026, effective immediately.

The First SBR Amendment Directions were issued following a review of the regulatory framework applicable to NBFCs that do not avail public funds and do not have any customer interface[1], recognising that such entities, by their very nature, pose limited systemic and consumer risk. The Second SBR Amendment Directions were issued pursuant to a review of the methodology for identification of NBFCs-UL and the placement of Government owned NBFCs in various layers under the scale based regulatory framework.

Together, these amendments represent a significant recalibration of RBI's proportionate regulation of NBFCs, reducing the compliance burden on low-risk entities while simplifying the criteria for enhanced oversight of systemically important ones.

ANALYSIS

First Amendment Directions: Reclassification and Exemption Framework

Three-Category Classification: The First SBR Amendment Directions introduce a formal three-category classification framework for NBFCs based on their access to public funds and customer interface:

[1]*The term 'customer interface' means means interaction between the NBFC and its customers while carrying on its business.*

Unregistered Type I NBFCs

NBFCs not availing public funds and not having any customer interface, with asset size below INR 1,000 crore, exempt from registration requirements under Sections 45IA and 45IC of the RBI Act.

Type I NBFCs

NBFCs not availing public funds and not having any customer interface, with asset size of INR 1,000 crore or above, registration with RBI as Type I NBFC is mandatory.

Type II NBFCs

NBFCs that avail public funds and/or have customer interface, regardless of asset size, registration with RBI as Type II NBFC is mandatory.

Conditions for Exemption: To qualify as an Unregistered Type I NBFC, the following cumulative conditions must be satisfied on an ongoing basis:

- The entity operates without public funds and without customer interface as its conscious and long-term business model
- Its asset size is below INR 1,000 crore as per the latest audited balance sheet
- It passes an annual Board resolution at the beginning of each financial year confirming that it will not avail public funds or have customer interface during the year
- It discloses its status as an Unregistered Type I NBFC along with status of public funds and customer interface in the Notes to Accounts of its financial statements

Key Definitional Clarifications: The First SBR Amendment Directions clarify that indirect receipt of public funds, i.e., funds received through associates and group entities which have access to public funds, also constitutes "public funds". The definition of "customer interface" encompasses any customer-oriented activity including lending, provision of guarantees, placement of inter-corporate deposits (including to group entities, shareholders and directors) and provision of any other product or service.

Group-Level Asset Aggregation: Where a group has multiple Unregistered Type I NBFCs, the asset size of all such entities must be aggregated. If the aggregate asset size reaches INR 1,000 crore or above, all Unregistered Type I NBFCs within the group are required to register as Type I NBFCs.

Deregistration Process: Existing NBFCs that qualify as Unregistered Type I NBFCs may apply for deregistration through the PRAVAAH portal by 31 December 2026. The application must be accompanied by audited financials for the last three financial years, a statutory auditor's certificate confirming the absence of public funds and customer interface, a Board resolution and an undertaking to disclose Unregistered Type I NBFC status in the Notes to Accounts.

Overseas Investment Restriction: Unregistered Type I NBFCs intending to undertake overseas investment in the financial services sector must register with RBI as Type I NBFCs.

Second Amendment Directions: Revised NBFC-UL Identification

Simplified Identification Criterion: The Second SBR Amendment Directions replace the erstwhile parametric scoring-based methodology for identifying NBFC-ULs with a single, asset-size-based criterion. The Upper Layer now comprises NBFCs with an asset size of INR 1,00,000 crore and above as per the latest audited balance sheet. The criteria for identification of NBFC-ULs shall be reviewed by RBI every three years.

Inclusion of Government Owned NBFCs: The Second SBR Amendment Directions bring Government-owned NBFCs within the purview of the scale based regulatory framework for the first time. However, Government-owned NBFC-ULs are exempt from mandatory listing and pre-listing disclosure requirements.

NBFC Group Entities of SCBs: NBFCs that are group entities of a SCB are required to adhere to the applicable provisions of the Reserve Bank of India (Commercial Banks – Undertaking of Financial Services) Directions, 2025, where a particular business or activity is being undertaken by both the NBFC and its parent bank.

Key Takeaways

The First and Second SBR Amendment Directions collectively reflect RBI's risk-proportionate philosophy: concentrate supervision on entities posing systemic risk, while easing the burden on closed-loop NBFCs with no public funds or external customers. The simplified NBFC-UL identification, replacing subjective parametric scoring with a bright-line INR 1,00,000 crore threshold reviewed every three years, provides greater certainty.

Eligible NBFCs should promptly evaluate their classification and, where applicable, initiate deregistration through the PRAVAAH portal before the 31 December 2026 deadline. Large promoter groups must map their NBFC footprint to assess group-level registration triggers.

The Conduct Code: Rewriting the Rules of Sale

BACKGROUND

The RBI amended its Responsible Business Conduct Directions in June 2026 via the Responsible Business Conduct Amendment Directions. Taking effect from 1 January 2027, the Responsible Business Conduct Amendment Directions set out a dedicated framework governing the advertising, marketing and sale of financial products and services by REs, including the engagement of DSAs and DMAs.

ANALYSIS

Policy and Code of Conduct: REs must adopt a board-approved policy covering advertising, marketing, and sale of their own products / services and TPPS, addressing aspects regarding suitability and appropriateness criteria, customer feedback mechanism, and compensation for mis-selling. Where DSAs / DMAs are engaged, the policy must also cover their eligibility, due diligence, training, performance standards, inspection and audit, control mechanisms, and penal actions for non-compliance. A separate Code of Conduct covering employees, DSAs / DMAs, their sub-agents and TPPS providers must be adopted, backed by signed undertakings, and published on the RE's website.

DSA / DMA Governance and Disclosure: DSAs / DMAs are broadly defined to include any external person engaged to sell, market or influence customers on an RE's behalf. REs must publish and keep updated (within seven calendar days of any change) a list of empaneled DSAs / DMAs on their website, ensure relevant personnel hold the prescribed qualifications, and make agents present on RE premises clearly identifiable from employees. DSAs / DMAs must deal with customers transparently and fairly, restrict customer contact to between 09:00 and 19:00 hours (absent contrary customer consent), disclose fees and rates upfront, honor customers' 'Do Not Disturb' preferences, and refrain from misrepresentation or unauthorized commitments.

Consent Architecture: Products may be sold only with the customer's explicit, informed consent, captured through defined modes such as a signed declaration, OTP, or digitally recorded confirmation. Where a form covers multiple products, each must be separately enumerated so customers can select only what they want. Consent interfaces must be designed to require review of the applicable terms and conditions before consent can be given, and the default option must be set to 'No'. Key product features, such as fees, interest, risks, lock-in and exit terms, must be prominently disclosed (using prescribed formats such as the KFS or MITC where applicable), and consent records retained for one year after the contract ends.

Suitability, Appropriateness and Documentation: REs must assess a product's suitability for a customer based on its features and risk profile, weighed against the customer's age, income and risk tolerance, following any sector-specific methodology where one is prescribed. Application forms, physical or digital, must clearly distinguish each product on offer and capture consent separately for each, with related documents made available in a language the customer understands. REs must acknowledge receipt of an application and provide the signed agreement to the customer securely on completion of the sale.

Prohibition on Mis-selling and Compulsory Bundling: Mis-selling is defined to include selling an unsuitable product (even with consent), selling on incomplete or misleading information, selling without explicit consent, compulsory bundling, and any other practice the relevant regulator specifies. REs must not incentivize mis-selling of TPPS, and compulsory bundling of a TPPS with an RE's own product is prohibited. However, customers may still be required to obtain a risk-mitigant product (such as loan insurance) as long as they remain free to choose the provider, and genuinely voluntary or complimentary bundles are not treated as bundling. REs also cannot fund a product purchase out of a sanctioned loan facility without the customer's explicit consent.

Prohibition on Dark Patterns: REs must ensure that their interfaces, as well as the interfaces of DSAs / DMAs engaged by them, do not deploy dark patterns (such as false urgencies, subscription traps, bait-and-switch, trick wording, etc.), and interfaces must be subjected to user testing and periodic internal audit to identify unfair features. Adherence to the CCPA's Guidelines for Prevention and Regulation of Dark Patterns, 2023 is mandatory.

Advertising and Sale of TPPS: All advertising and promotional materials, physical or digital, pertaining to TPPS must be clear and factual and disclose the interest rate and associated fees, with terms and conditions prominently displayed at all points of sale and digital channels. Promotional communications may be sent only to customers who have provided explicit consent to receive them, and the unsubscribing process must be easy and simple. An RE is not allowed to advertise TPPS as its own and must clarify its role when presenting any TPPS provider's product.

Interface with Other Regulatory Regimes: REs must comply with adjacent regulatory frameworks, including the TRAI / DoT commercial-communication rules (TCCCPR as amended), the product-specific requirements of SEBI, IRDAI, and PFRDA, and the RBI's own guidelines on agency business, outsourcing, and deposit mobilization through agents.

Key Takeaways

REs must adopt comprehensive policy covering advertising, marketing, sale, suitability and appropriateness, customer feedback, and mis-selling compensation, extending to the governance of DSAs / DMAs.

Consent architecture will need to be re-engineered to incorporate explicit, product-wise consent, a default 'No' setting, mandatory review of terms and conditions before consent, one-year record retention.

DSA / DMA arrangements must comply with the RE's Code of Conduct and undertakings and must be publicised on the RE's website.

Product suitability assessment must be embedded into sale journeys.

REs must establish a robust customer grievance redressal, feedback and compensation mechanism for mis-selling, with half-yearly reporting requirements.

User interfaces must be tested and audited for dark patterns.

NBFC of all Trades, Master of None

BACKGROUND

On 15 June 2026, RBI issued the UFS Second Amendment Directions, overhauling the framework governing agency business and third-party product distribution by NBFCs, including HFCs. The UFS Second Amendment Directions revise the UFS Directions (Existing Directions) and follow draft amendments circulated for public consultation in February 2026.

Issued alongside parallel amendments to the Reserve Bank of India (Non-Banking Financial Companies – Responsible Business Conduct) Directions, 2025 (NBFC RBC Directions), the two sets of directions establish a two-layer architecture: the financial services framework operates as the permission layer (determining what distribution arrangements are permissible), while the RBC framework serves as the conduct layer (governing how the NBFC must behave in executing those arrangements).

The Amendment Directions come into effect on 1 January 2027.

ANALYSIS

Unified definition of "Agency Business" and restricted regulatory perimeter: The UFS Directions had no consolidated definition of agency business. Insurance distribution, mutual fund distribution and pension fund services each operated under separate product-specific regimes. The UFS Second Amendment Directions consolidate these into a single agent–principal framework: agency business is now defined as an arrangement where the NBFC acts as agent of a TPPSP, without risk participation, to facilitate the sale of the TPPSP's products to the NBFC's own customers (covering marketing, sales, promotion, grievance facilitation and after-sale services).

Crucially, the UFS Second Amendment Directions introduce a defined category of "Regulated financial products and services" (products falling under the regulatory ambit of RBI, SEBI, IRDAI, PFRDA or overseas authorities including IFSCA) and restrict agency business exclusively to products within this perimeter. NBFCs can therefore no longer distribute unregulated products through agency arrangements, a material tightening from the draft amendments, which did not contain this restriction.

Referral services, a notable gap: For commercial banks, RBI has introduced a specific "Referral Services" arrangement allowing a bank to refer customers to a TPPSP by sharing product information, without undertaking distribution, grievance redressal or post-sale services. No equivalent provision exists for NBFCs. The TPPSP definition acknowledges the concept of a "referral arrangement," but the operative text grants no permission to undertake one. NBFCs operating referral-type arrangements will need to assess whether these retain a proper regulatory footing under the revised framework.

Uniform conditions across distribution activities: In place of the fragmented product-specific regimes, the UFS Second Amendment Directions prescribe a single set of conditions applicable uniformly to insurance, mutual fund and pension fund distribution:

- Compliance with the relevant product regulator (IRDAI, SEBI or PFRDA)
- Full compliance with the NBFC RBC Directions
- A fee-basis arrangement without risk participation, with fees disclosed upfront
- The TPPSP must maintain robust grievance redressal mechanisms
- Product display on digital channels is restricted to products covered under the arrangement.

Notably, under the UFS Directions, pension distribution was not expressly required to be conducted on a fee basis without risk participation. The UFS Second Amendment Directions now impose this condition, aligning pension distribution with the standard already applicable to insurance and mutual fund agency. Additionally, for insurance distribution, the prior requirement that premiums not be routed through the NBFC has been removed.

Migration of conduct provisions to the RBC framework: The UFS Second Amendment Directions transfer detailed conduct requirements from the UFS Directions to the NBFC RBC Directions, including Board-approved policy requirements, customer suitability assessments, commission and incentive restrictions, disclosure obligations and grievance redressal. The change is structural rather than substantive with the underlying obligations persisting, but compliance being required to be tracked under the RBC framework.

Key Takeaways

Comprehensive review required: NBFCs should review existing agency arrangements, digital distribution journeys and commercial terms with TPPSPs to ensure alignment ahead of the 1 January 2027 effective date.

Digital distribution and embedded finance: NBFCs cannot display an open marketplace of unregulated products. In-app insurance or mutual fund purchase journeys must fall within the agency framework and comply with the full conduct layer under the NBFC RBC Directions.

Revenue model impact: The uniform "fee basis without risk participation" standard, particularly for pension distribution arrangements which did not previously require this, may necessitate renegotiation of commercial terms with TPPSPs. Commission-based incentive structures for staff and DSAs / DMAs will also require revision under the NBFC RBC Directions.

Anti-bundling implications: The NBFC RBC Directions, to which the UFS Second Amendment Directions are expressly linked, introduce an explicit prohibition on compulsory bundling of third-party products with the NBFC's own products (such as requiring insurance purchase as a condition for loan approval) and mandate specific customer consent before any third-party product is

sold. These provisions, read with the fee-basis requirement under the UFS Second Amendment Directions, are intended to close the regulatory arbitrage previously exploited in credit-linked insurance distribution.

Multi-regulator compliance: Distribution activities are conditioned on simultaneous compliance with the relevant product regulator and the RBI's structural and conduct requirements. NBFCs should map both sets and identify conflicts, particularly on commission structures and documentation requirements.

Brick, Mortar and Credit: Banks open the Door to REIT Lending

BACKGROUND

RBI issued the Third SCB Credit Amendment Directions on 10 June 2026, amending the SCB Credit Directions. The Third SCB Credit Amendment Directions introduce a comprehensive framework for bank lending to REITs and harmonise the existing framework for lending to InvITs. The Third SCB Credit Amendment Directions become effective on 1 October 2026, or an earlier date if adopted by an SCB in its entirety.

REITs had until now lacked access to bank credit, despite being SEBI-regulated, listed investment vehicles with income-generating real estate portfolios. The existing InvIT lending framework also lacked detailed prudential safeguards suited to trust-based investment vehicles.

ANALYSIS

Core eligibility criteria: SCBs are now permitted to lend to SEBI-registered REITs and InvITs that are listed on recognised stock exchanges. For REITs, at least 80% of the trust's underlying assets must be generating positive cash flow from operations for not less than one year. For InvITs, at least 80% of the value of the trust's assets must be invested in completed and revenue-generating infrastructure projects generating net positive cash flows from operations for not less than one year. SCBs may not use REIT or InvIT lending to fund SPVs that have existing loans from REs and are facing financial difficulty.

Board-approved policies and end-use monitoring: Banks must adopt a Board-approved policy on lending to REITs and InvITs covering appraisal mechanisms, sanctioning conditions, underwriting norms (including debt service coverage ratio benchmarks), internal exposure limits and monitoring mechanisms. Banks must also strictly monitor the end use of funds to ensure lending is not used to finance activities not directly permitted under extant regulations.

Repayment structures and refinancing: Credit facilities extended to REITs and InvITs must not involve bullet or ballooning repayment structures, ensuring that a disproportionate portion of principal repayment is not concentrated in the terminal phase of the loan tenure. This restriction does not apply to SCB exposures through investments in bonds, debentures and commercial paper. Refinancing of existing SPV credit facilities is restricted to completed projects, i.e.:

- In the case of REITs, projects that have received a completion certificate, occupancy certificate or equivalent

- In the case of InvITs, projects that have achieved commencement of commercial operations.

Prudential ceilings on leverage and exposure: The overall leverage of a borrowing REIT or InvIT must remain within the prudential ceiling prescribed by SEBI, or such lower limit as the SCB's Board may determine. The aggregate exposure of all SCBs to a borrowing REIT or InvIT, together with its underlying SPVs and holding companies, is capped at 49% of the gross value of the trust's assets, determined without netting cash and cash equivalents.

Security coverage and lender protection: SCB financing must be fully secured by, inter alia, a charge over the underlying immovable property, an assignment of cash flows and receivables, a pledge of equity interests held by the trust in the relevant SPV and other legally enforceable security interests. Any charge over immovable property must be an exclusive first charge, or a first pari passu charge governed by an inter-creditor agreement where multiple lenders are involved.

For REITs specifically, a mortgage over immovable property is mandatory wherever financing is extended for acquisition or development of a property, including indirect acquisitions through purchase of equity in an SPV or holding company. Loan agreements must provide for robust lender protection, including mandatory escrow arrangements for cash flow ring-fencing and restrictions on the borrower and underlying SPVs from availing additional debt without existing lender consent.

Acquisition finance and transitional provisions: SCB finance utilised by REITs or InvITs for acquiring stakes in other entities, including SPVs and holding companies, is subject to the conditions under Chapter XI (Acquisition Finance) of SCB Credit Directions, with targeted exemptions such as waiver of net-profit history requirements and non-financial target restrictions. Existing InvIT loans that do not conform to the amended framework as on the effective date may run off till maturity; however, SCBs may not review, renew or enhance such limits unless they comply with the amended framework.

Key Takeaways

The Third SCB Credit Amendment Directions open bank credit as a new funding channel for listed REITs, alongside existing capital market instruments, while bringing enhanced clarity and more prescriptive prudential safeguards to the InvIT lending framework.

SCBs should prioritise the following ahead of the effective date:

Board-approval of either dedicated REIT and InvIT lending policies or inclusion of provisions in relation to financing REITs and InvITs in the existing credit policy of the SCB

Development of internal exposure limits aligned with the amended regulatory framework

Updation of loan documentation templates to incorporate the mandated security package, escrow arrangements and debt-issuance restrictions

Assessment of existing InvIT portfolios to identify exposures requiring run-off treatment

02

PAYMENTS

India's digital payments ecosystem has grown rapidly over the past decade, but the last year has been the most significant from a regulatory standpoint. The phase of rapid adoption and volume growth has given way to one of consolidation, where the RBI is focused on bringing scattered frameworks together, plugging gaps, and making sure the infrastructure is strong enough for the next level of scale. UPI volumes continue to grow in double digits, credit on UPI is picking up, and digital payments are reaching deeper into tier two and tier three markets. But with scale has come a sharp rise in fraud, making security and trust the dominant themes of the year.

The biggest shift has been the RBI's decision to bring all forms of payment aggregation, whether online, offline or cross border, under one unified framework. For years, offline aggregation sat in a grey zone and cross border payments ran on a different set of rules. That is now over. The RBI treats payment aggregation as a single regulated activity regardless of channel, and expects uniform standards of governance, merchant checks, fund management and cyber resilience across the board.

At the same time, the authentication layer is being upgraded beyond SMS-based OTPs, with an emphasis on interoperability, open access and risk-based approaches. On prepaid instruments, the direction is towards tighter controls, stronger consumer protection (particularly around unused balances), and a clear signal that low KYC instruments are not meant for routine or long-term use.

For payments businesses, the message is straightforward: the days of operating in grey areas or relying on gaps between frameworks are done. The regulatory perimeter is well defined, compliance expectations are specific, and transition timelines are tight. Businesses that have invested early in governance and security infrastructure will be well placed; those that do not will need to move quickly.

Offline, Online, in Line: Payment Aggregators Under One Roof

BACKGROUND

On 15 September 2025, the RBI issued the PA Directions as a Master Direction under the PSS Act and FEMA. The PA Directions rationalise and repeal the erstwhile framework, comprising the Guidelines on Regulation of Payment Aggregators and Payment Gateways dated 17 March 2020, the related clarifications dated 31 March 2021, the Regulation of Payment Aggregator – Cross Border directions dated 31 October 2023, and certain ancillary operational circulars.

Building on the two draft directions released for public consultation in April 2024, the PA Directions bring physical (offline) payment aggregation squarely within RBI's regulatory perimeter for the first time, harmonise the three categories of PAs under a single framework, and introduce more stringent merchant due diligence, governance and security obligations. The PA Directions apply to all bank and non-bank entities undertaking PA business, and to AD Banks and SCBs that engage with such entities.

ANALYSIS

Definitions and Categories of PA: A PA is defined as an entity that facilitates aggregation of payments made by customers to merchants, through one or more payment channels via the

merchant's interface (physical or virtual), for the purchase of goods, services or investment products, and subsequently settles the collected funds to such merchants.

PAs ARE CLASSIFIED INTO THREE CATEGORIES:

- PA-O, where the acceptance device and payment instrument are not in close proximity
- PA-P, where both are physically present in close proximity
- PA-CB, which facilitates cross-border aggregation of permitted current account transactions via e-commerce, with separate sub-categories for inward and outward transactions.

"Merchant" has been broadened to expressly include marketplaces, exporters, overseas sellers and entities offering investment products. A PG, which routes payment transactions without handling funds, falls outside the scope of the PA Directions, though PGs are encouraged to adopt the baseline technology recommendations prescribed for PAs.

Authorisation, Capital and Governance: Consistent with the erstwhile regime, banks do not require separate authorisation, while non-bank entities must be incorporated in India as a company under the Companies Act and seek authorisation from RBI through its online portal (with an NOC from any other financial sector regulator, where applicable). Minimum net-worth thresholds remain unchanged: INR 15 crore at application, rising to INR 25 crore by the end of the third financial year, maintained on an ongoing basis and certified by the statutory auditor. An existing PA already carrying on PA-P business must intimate RBI to obtain a revised CoA, and an entity carrying on only PA-P business (or with a pending PA-O / PA-CB application) must apply for authorisation by 31 December 2025, failing which it must wind up its PA-P business by 28 February 2026. A PA must be professionally managed, with promoters and directors satisfying 'fit and proper' criteria at all times, and any change in control of a non-bank PA requires RBI's prior approval.

Conduct of Business, Disputes and Security: A PA must maintain a dispute resolution mechanism for payment-related disputes, including refund timelines and adherence to RBI's TAT instructions for failed transactions, and appoint a grievance officer with a publicly displayed escalation matrix. On security, a PA must implement adequate information and data security infrastructure, ensure merchant compliance with standards such as PCI-DSS and PCI-SSF, adopt a Board-approved Information Security Policy, and undergo an annual system and cyber security audit by a CERT-In empanelled auditor, in line with RBI's Cyber Resilience Master Directions.

Specific Directions for PA-CB: Funds relating to inward and outward transactions must be kept strictly separate, with no co-mingling or netting-off permitted. For outward transactions, a PA-CB may directly onboard overseas merchants or contract with overseas e-commerce marketplaces, using any authorised payment instrument other than a small PPI. Foreign currency may only be bought or sold through an AD bank, and the maximum value per transaction is capped at INR 25 lakh. Settlement in non-INR currencies is permitted only for Indian exporter-merchants directly onboarded by the PA-CB facilitating inward transactions.

Know Your Customer and Due Diligence: A PA must undertake CDD of its merchants under the applicable KYC framework, retrieving the merchant's record from the CKYRC as the first port of call, with other modes available only where the record is unavailable or outdated. A lighter-touch process applies to merchants with annual turnover up to INR 40 lakh, or export turnover up to INR 5 lakh. A PA must also conduct background checks, ensure funds are credited only to the merchant's own account, and monitor transactions against the merchant's business profile. Non-bank PAs must register with the FIU-IND. Agents may only be used for digital KYC and assisted V-CIP, with ultimate responsibility remaining with the PA.

Settlement of Funds and Escrow Accounts: Domestic PAs (PA-O and PA-P) must maintain an escrow account with an SCB, while a PA-CB must maintain separate InCA and OCA with an AD Bank, used only for authorised PA business and compliant by 31 December 2025. Pre-funding and inter-escrow transfers are permitted for the domestic escrow account but not InCA, and permitted credits and debits now expressly recognise inter-PA settlements, with third-party debits on a merchant's instruction subject to turnover-linked conditions.

Key Takeaways

The PA Directions consolidate a fragmented framework and, for the first time, subject PA-P entities to a licensing and supervisory regime on par with PA-O and PA-CB, with a firm 31 December 2025 authorisation deadline and 28 February 2026 wind-up deadline for non-compliant PA-P entities. The new governance, security and reporting obligations are a consequential shift: PAs are now directly responsible for fit and proper standards, Board-level information security governance, CERT-In audited cyber resilience, and enhanced merchant due diligence, with merchants onboarded before 31 December 2025 requiring compliance by 15 September 2026.

The recalibrated escrow architecture, distinguishing domestic escrow accounts from InCA and OCA, will require PAs to revisit treasury and settlement processes. Businesses that had housed offline aggregation in a separate entity may wish to reassess their corporate structure, and PAs should ensure their governance frameworks, security policies, onboarding processes and contracts are aligned well ahead of these transition deadlines.

Trust, but Verify: RBI's New Rules for AEPS Operators

BACKGROUND

On 27 June 2025, the RBI issued the AePS Directions to all SCBs (including RRBs), UCBs, state and district central cooperative banks, and the NPCI. AePS, operated by NPCI, facilitates interoperable transactions using Aadhaar-enabled biometric or OTP authentication, offering financial services such as cash withdrawal, cash deposit and fund transfer. It has emerged as a cornerstone of financial inclusion, with more than 37 crore users transacting through it in 2023.[2] However, rising instances of fraud perpetrated through identity theft and the compromise of customer credentials prompted the RBI to take measures aimed at enhancing system robustness.

Having first flagged this concern in its Statement on Developmental and Regulatory Policies dated 8 February 2024, the RBI has now moved to streamline the onboarding of ATOs and strengthen fraud risk management. Issued under Section 18 read with Section 10(2) of the PSS Act, the AePS Directions came into effect from 1 January 2026.

ANALYSIS

Due Diligence at Onboarding: Acquiring banks must carry out due diligence of every ATO before onboarding, adopting the CDD process for individuals stipulated under the applicable KYC framework prescribed by the RBI. Where an ATO's due diligence has already been completed in its capacity as a business correspondent or sub-agent, the same may be relied upon. Acquiring banks are also required to undertake periodic updation of the ATO's KYC.

KYC of Inactive Operators: Where an ATO has not performed any financial or non-financial transaction for a customer for a continuous period of three months, the acquiring bank must refresh the operator's KYC before enabling him or her to transact further.

Ongoing Risk Management: Acquiring banks must monitor the activities of ATOs through their transaction monitoring systems on an ongoing basis and set operational parameters based on each operator's business risk profile. Aspects such as the location and type of the ATO and the volume and velocity of transactions must form part of the bank's fraud risk management framework, and these operational parameters must be reviewed periodically to reflect emerging fraud trends.

System-Level Controls: Acquiring banks must put in place adequate system-level controls to ensure that any technological integrations, such as APIs, are used only for enabling AePS operations.

[2] *Reserve Bank of India, Statement on Developmental and Regulatory Policies (8 February 2026).*

Key Takeaways

The directions squarely place the onus of gatekeeping the AePS ecosystem on acquiring banks, reflecting the RBI's continued emphasis on robust safeguards around touchpoint operators who serve vulnerable customers in rural and underserved areas. Acquiring banks need to ensure that their onboarding workflows, transaction monitoring systems and API governance comply with the AePS Directions.

Acquiring banks will also need to review their contractual arrangements with business correspondents and ATOs to ensure these clearly allocate responsibility for onboarding due diligence and periodic KYC updation, embed audit and transaction-monitoring rights, and restrict API usage to AePS operations, so that the contractual framework keeps pace with the RBI's tightened due diligence and risk management expectations.

By anchoring ATO onboarding to the applicable CDD standards and mandating dynamic, risk-based transaction monitoring, the RBI seeks to curb identity-theft driven frauds while preserving the central role AePS plays in financial inclusion.

Factor Check: India's Authentication Framework Gets an Upgrade

BACKGROUND

The Digital Payment Authentication Directions were issued on 25 September 2025 to standardise authentication mechanisms for banks and non-bank PSPs that process domestic digital payment transactions. Prior to the Digital Payment Authentication Directions, digital payments were already required to have 2FA, with most REs opting for SMS-based OTPs as the additional factor, although no specific factor had been mandated. The Digital Payment Authentication Directions must be complied with by 1 April 2026.

ANALYSIS

Classification of Factors of Authentication: The Digital Payment Authentication Directions classified the factors of authentication that PSPs may deploy into three broad user-based categories:

- Possession-based (such as software tokens or card hardware)
- Knowledge-based (such as a PIN, passphrase or a password)
- Identity-based (such as fingerprint or any other biometric data)

Mandatory 2FA: All issuing REs and PSPs are now required to maintain 2FA at a minimum, except for certain types of exempted transactions (such as small-value contactless card-based transactions up to INR 5,000, recurring transactions, gift PPIs, PPIs for MTS, small-value digital payments made in offline mode up to INR 500, NETC transactions,

and specified travel bookings made through commercial / corporate cards). Issuers may, at their discretion, offer their customers a choice of authentication factors. Further, the authentication mechanism must be robust, comprising independent authentication factors such that a compromise in one factor does not result in the compromising of the other factor.

Dynamic Factor: At least one of the factors of authentication must be dynamically generated or proven (such as SMS-based OTP or biometric verification), except for card present transactions.

Interoperability and Open Access: All authentication mechanisms / solutions which are developed / deployed by issuing REs and PSPs must be accessible to all applications / token requestors functioning in that operating environment for all use cases / channels or token storage mechanisms.

Transaction Risk Identification: Issuing REs and PSPs may also identify and evaluate certain transactions based on parameters such as transaction location, user behaviour patterns, device attributes and historical transaction profile. Where a transaction is deemed high-risk, issuers may require additional authentication factors beyond the minimum two, subject to their internal risk management policies, and may explore using DigiLocker as a platform for notification and confirmation of such high-risk transactions.

Responsibility of the Issuer: An issuer must ensure the robustness and integrity of the authentication mechanism before deployment. If any loss arises out of transactions effected without complying with the Digital Payment Authentication Directions, the issuer must compensate the customer for the loss in full.

Issuers must also ensure adherence to the provisions of the DPDP Act.

Compliance Requirements for Cross-border CNP Transactions: While the Digital Payment Authentication Directions apply only to domestic digital payments, card issuers are required to establish:

- A mechanism to validate non-recurring, cross-border CNP transactions where request for authentication is raised by an overseas merchant or overseas acquirer
- A risk-based mechanism for handling all cross-border CNP transactions by 1 October 2026. Card issuers must also register their BINs with card networks

Key Takeaways

All issuing REs and PSPs must maintain at least 2FA for domestic digital payments, using independent factors drawn from the possession-based, knowledge-based and identity-based categories.

At least one authentication factor must be dynamically generated or proven, except for card present transactions. This allows REs and PSPs to move beyond sole reliance on SMS-based OTPs and adopt alternatives such as biometric verification.

Authentication solutions must be interoperable and openly accessible to all applications and token requestors in the operating environment. REs and PSPs cannot deploy closed or proprietary authentication mechanisms.

REs and PSPs may adopt risk-based authentication, applying additional factors to transactions identified as high-risk based on relevant parameters, and may explore DigiLocker for notifying and confirming such transactions.

Issuing REs will be liable to fully compensate customers for losses arising from transactions effected without complying with the Directions, making robust compliance essential. Issuers must also ensure the integrity of the authentication mechanism before deployment and comply with the DPDP Act.

With the Digital Payment Authentication Directions becoming effective from 1 April 2026, REs and PSPs should review and upgrade their existing authentication systems to ensure timely compliance.

Reloaded: RBI's Proposed Rulebook for Prepaid Instruments

BACKGROUND

On 22 April 2026, the RBI issued the Draft PPI Directions, following a comprehensive review of the extant Master Directions on Prepaid Payment Instruments, 2021. The Draft PPI Directions are stated to be issued under the Payments Vision 2025 framework, pursuant to the PSS Act. The Draft PPI Directions aim to strengthen the security of PPIs in India, with tighter controls on issuance, operational features, and monthly transfer limits, while streamlining certain compliance and approval requirements for PPI issuers.

ANALYSIS

Definition and categorisation of PPIs: The definition of PPI is broadened to cover the facilitation of transactions generally, while clarifying that stored value does not include digital currency. The formal "Closed System PPI" category is done away with, though the exemption from RBI authorisation is preserved for such PPIs issued by any entity other than a "marketplace" (aligned with the definition under the RBI PA Directions. Consequently, PPIs used for purchases on marketplace platforms must now be issued by a licensed PPI issuer. The Draft PPI Directions also remove the requirement for a board-approved PPI policy, simplifying issuance governance for authorised entities.

Authorisation and Capital Requirements: Banks permitted to issue debit cards may issue PPIs with prior intimation to RBI, while non-bank entities must apply for authorisation through RBI's online portal and be incorporated in India under the Companies Act. The minimum net worth for non-bank PPI issuers is INR 5 crore at the time of application, rising to INR 15 crore by the end of the third financial year of authorisation, to be maintained on an ongoing basis. Promoters and directors must satisfy 'fit and proper' criteria at all times, and any change in control of a non-bank PPI issuer requires RBI's prior approval.

Full KYC PPIs: Each issuer is now restricted to issuing only one Full KYC PPI per holder. A new overall monthly debit limit of INR 2,00,000 is introduced, with P2P transfers capped separately at INR 25,000 per month (replacing the earlier cap of INR 10,000 per month with an enhanced limit of INR 2,00,000 for pre-registered beneficiaries). Cash loading to Full KYC PPIs is reduced from INR 50,000 to INR 10,000 per month. The explicit cash withdrawal limits under

the PPI MD (INR 2,000 per transaction and INR 10,000 per month) are removed; withdrawals are now subject to extant RBI regulations.

Small PPIs: Small PPIs now carry a hard maximum validity of two years, after which the outstanding balance must be transferred back to the source account; no further Small PPI may be issued to the same holder after expiry. The earlier distinction between Small PPIs with and without cash loading facility is removed. Small PPIs are to be issued only where CDD cannot be completed. Read alongside the validity and re-issuance restrictions, the regulatory intent appears to be to curtail the routine use of Small PPIs.

Loading, expiry and inactivity: Credit card loading is now limited to Special Purpose PPIs only. Loading through agents is restricted. Banks may load PPIs only through BCs, while non-banks may use 'agents in person' under the PSO Outsourcing Framework dated 3 August 2021. A PPI issuer must close the PPI after one year of inactivity, without any explicit notice requirement (though notice at reasonable intervals during the 45 days prior to expiry/ inactivity is mandated).

Critically, outstanding balances from closed PPIs must be credited back to the source account or a verified bank account of the holder. PPI issuers will no longer earn 'breakage revenue' from unspent balances, which is particularly significant for Gift PPIs, promotional wallet credits, and dormant PPIs that aggregated represent material revenue for large issuers.

Special Purpose PPIs: Gift PPIs now prohibit cash purchases and carry a maximum validity of one year. PPIs for Foreign Nationals and NRIs carry a revised monthly debit limit of INR 5,00,000, are issued after physical verification of Passport and Visa, and are closed on Visa expiry with unutilised balance transferred back to source (refund in foreign currency permitted, subject to compliance with the FEMA). Transit PPIs retain perpetual validity with a balance cap of INR 3,000.

Co-branding arrangements: The requirement for one-time RBI approval for non-banks entering co-branding arrangements is removed, as are the requirements for a board-approved co-branding policy and prominent display of the PPI issuer's name on the instrument. The erstwhile restriction requiring only the bank to act as PPI issuer in a bank / non-bank arrangement is also removed. The co-branding partner's role remains limited to marketing and distribution, and the PPI issuer remains fully liable for all acts of the partner. Given continuing full liability, issuers would be prudent to maintain voluntary internal governance frameworks.

Cross-border transactions: The Draft PPI Directions prohibit the use of PPIs for any cross-border transactions (previously, INR-denominated PPIs could be used for certain outward trade transactions up to INR 10,000 per transaction and inward remittances under the Money Transfer Service Scheme). This represents a significant tightening that may impact fintech business models relying on PPI-based cross-border payment flows.

Miscellaneous compliance easing: The requirement to submit the list of acquired merchants to the escrow bank is removed. The obligation to retain transaction logs for at least ten years is removed. The calculation of the 'core portion' of the escrow account eligible to earn interest is simplified to a monthly basis (previously fortnightly). Non-bank PPI issuers continue to maintain funds in a separate escrow account with an SCB, with statutory auditor certification on a quarterly basis.

Customer Protection and Interoperability: A PPI issuer must disclose all PPI features, charges, validity and terms in clear and simple language (preferably English, Hindi and the local language) and put in place a publicly disclosed grievance redressal framework, including a nodal officer and escalation matrix. Holders have recourse to the Reserve Bank Integrated Ombudsman Scheme, 2026. PPI issuers must comply with RBI's TAT and ODR instructions, and liability for unauthorised transactions is governed by the applicable responsible business conduct directions (except for offline payments). Full KYC PPI holders must be enabled to transact through a card network or the UPI on the issuer side.

Key Takeaways

The Draft PPI Directions represent a significant recalibration of India's PPI regulatory framework, tightening controls on issuance and transaction limits while materially reducing compliance, reporting, and approval burdens on issuers. Consumer protection remains a clear regulatory priority, as reflected in the mandatory closure and refund obligations for inactive PPIs and the elimination of breakage revenue. Operational flexibility has been extended to issuers in several areas, particularly in relation to co-branding and board governance requirements.

The RBI has not presently contemplated any transition period for issuers to comply with the Draft PPI Directions; a reasonable implementation timeline, along with clarity on other operational aspects (including the treatment of reloading and the meaning of 'agents in person'), would be beneficial for the industry. Issuers should review existing arrangements, including co-branded card portfolios, and take steps to consolidate or close multiple PPIs held by a single holder. The bifurcated limit structure (overall debits and P2P transfers) imposes a dual monitoring obligation, and the reduction in cash loading limits may pose difficulties in cash-heavy, semi-rural, and rural contexts.

03

DATA GOVERNANCE AND RISK MANAGEMENT

Data has become the lifeblood of India's financial system. It is the invisible current that sustains every critical function of the modern regulated entity. From the calculus of credit underwriting to the detection of fraud, from customer onboarding to regulatory reporting, virtually every operation performed by contemporary financial institutions draws upon data as its essential substrate. This dependence has accelerated with the march of digitalisation: the proliferation of digital lending, thenationwide expansion of UPI, and the embrace of artificial intelligence and machine learning have elevated data from back-office resource to strategic asset of the first order.

Recognising the magnitude of this transformation, the RBI has moved with purpose to establish a comprehensive governance architecture for data and the algorithmic models that depend upon it. The two draft guidances examined in this chapter—the Draft Data Governance Guidance and the Draft MRMF—signal the RBI's unambiguous intent: to treat data governance and model risk not as peripheral compliance exercises, but as core institutional capabilities embedded in Board oversight and woven into the fabric of day-to-day operations.

The Draft Data Governance Guidance, drawing upon international standards including the BCBS Data Principles, mandates that every regulated entity formulate a Board-approved DGF. It prescribes designated data roles, SSOT for critical data elements, rigorous quality metrics, lifecycle management protocols, and stringent controls governing the sharing of data with third parties. For lending service providers, digital lending platforms, and fintechs whose business models depend upon data flows with regulated entities, the implications are far- reaching: contract renegotiation, technical upgrades, and enhanced audit capabilities will become operational imperatives.

The Draft MRMF addresses what transpires when data is fed into algorithms and decision engines. With the accelerating reliance upon AI and ML, the RBI has sounded a clear warning: poorly managed models can yield flawed decisions, financial losses, and compliance failures of systemic consequence. The Draft MRMF mandates a Board-approved Model Risk Management Framework encompassing model taxonomy, governance architecture, risk tiering, validation protocols, documentation standards, and lifecycle management—capturing not only sophisticated AI systems but also the humble spreadsheet-based calculators whose outputs influence credit terms and pricing.

For AI and ML models, the Guidance prescribes additional safeguards of particular rigour: explainability thresholds, bias and fairness assessments, adversarial testing, red-teaming exercises, controls for dynamic updates, and mandatory human oversight including kill-switch mechanisms. Customer-facing AI systems must disclose that the user is interacting with an artificial intelligence. Third-party models attract governance standards no less exacting than those developed internally—accountability, in the RBI's conception, does not diminish with outsourcing.

Both guidances must be read in conjunction with the DPDP Act. Whilst the DPDP Act concentrates upon consent frameworks and the rights of data principals, the RBI guidances extend their reach to all organisational data —per-

sonal and non-personal alike. The practical course for regulated entities will be to construct a unified data governance control layer capacious enough to accommodate both regimes, rather than to maintain parallel compliance architectures.

The message from the RBI is unequivocal: as India's financial system grows ever more data-intensive and algorithmically driven, the governance of data and models will determine which institutions can scale safely—and which cannot. These foundational requirements are no longer optional enhancements; they are the preconditions of institutional resilience in the digital age.

Every Byte Counts: RBI's Data Governance Blueprint

BACKGROUND

RBI issued the Draft Data Governance Guidance on 15 July 2026, setting out regulatory expectations for standardised data governance across all RBI-regulated entities (as used in this section, REs include SCBs, SFBs, payments banks, LABs, RRBs, UCBs, RCBs, NBFCs across all layers, AIFIs and other entities regulated by RBI). The Guidance recognises data as a strategic organisational asset and draws on international standards, including the BCBS Data Principles, to propose a framework covering data governance, roles and responsibilities, the data lifecycle, architecture and third-party arrangements.

ANALYSIS

Wide definition of Data: "Data" is defined broadly as any recorded concepts, facts, information, opinion or instructions, regardless of form or medium, suitable for communication, interpretation or processing by humans or automated means. This sweeping definition brings virtually all categories of information within the compliance perimeter, requiring REs to overhaul existing practices around data aggregation, processing, storage, transformation and disposal.

Data Governance Framework and Data Governance Committee: Every RE must formulate a DGF proportionate to its size, complexity, business model and IT / IS setup, reviewed annually or more frequently. The DGF must comply with the DPDP Act. Every RE must also constitute a Board-level DGC (or assign the role to an existing Board-level committee) to oversee DGF implementation and formulate and review data governance policies.

Data roles and responsibilities: REs must establish a dedicated Data Function headed by a sufficiently senior officer not below the rank of CGM or equivalent, acting as the central point of coordination. Three distinct roles must be designated:

Data Owners, accountable for governance outcomes within each data domain

Data Stewards, responsible for operationalising governance requirements;

Data Custodians, responsible for technical management including access controls, storage, backup, and disaster recovery.

Data classification and risk management: REs must classify data based on risk, criticality to business operations, criticality to customers, and business and financial impact, aligning with classifications used by other financial sector regulators. Data risk must be managed within the overall risk management framework, structured around principles of accountability, integrity, auditability, transparency, traceability, proportionality, and standardisation. Cross-border data operations must be managed such that they do not impair the RE's ability to access, retrieve, or manage its data; foreign banks and Indian banks with offshore operations will need to review policies and amend contracts with overseas group entities and offshore service providers to ensure retrieval, access and audit rights.

Data processing, sharing and minimisation: Any processing or sharing of data, internally or to third parties, must use approved rules, logic, and standards. REs must have valid business justification to share data even between departments, driving stringent data minimisation at allstages of the data lifecycle.

Data quality management: REs must identify and maintain SSOT identifiers for each data element, with reconciliation mechanisms to detect and correct mismatches. REs must maintain metadata and data lineage that travels with the data when it moves to other systems. Data quality metrics and persistent issues must be placed before the DGC at quarterly or more frequent intervals.

Third-party arrangements: REs remain responsible for governance of data shared with third parties, including group entities. Data may be shared only for defined and approved purposes, on a need-to-know basis, with traceability to the SSOT, non-disclosure clauses, ongoing monitoring, and periodic audits (including through CERT-IN empanelled auditors). Externally sourced data must meet the same governance standards as internal data. These provisions are particularly consequential for LSPs and digital lending platforms, which will be required to upgrade technical capabilities; existing agreements and flow-down obligations with technology service providers will need to be amended.

Alignment with DPDP Act and overlap with cybersecurity / IT norms: The Draft Data Governance Guidance is broader than the DPDP Act, but the DGF must comply with it. Its focus on consent management, permissible usage, classification, retention and secure disposal maps closely to DPDP Act concepts. The practical approach is for REs to build a common data governance control layer, with DPDP-specific controls sitting within it for personal data. The Guidance does not replace existing RBI cybersecurity and IT governance requirements but bridges cyber controls and

organisation-level data management. REs should integrate DGF requirements with existing cybersecurity, IT risk, outsourcing, business continuity and information security policies rather than build a standalone framework.

Key Takeaways

Nearly all data held by REs will fall within scope, requiring an overhaul of existing data practices. Data must now be treated as an asset that is owned, classified, tracked, risk-managed, quality-checked, and protected across its life cycle.

REs must build a DGF, constitute a Board-level DGC, establish a Data Function led by a senior officer (CGM or equivalent), and designate Data Owners, Data Stewards and Data Custodians.

REs must have valid business justification to share data even between departments, driving stringent data minimisation at all stages of the data lifecycle.

REs must maintain an SSOT, metadata and lineage, and report data quality to the DGC at least on a quarterly basis.

Third-party, LSP and group-entity data arrangements must be reviewed and amended for need-to-know access, audit and non-disclosure obligations, and flow-down terms. LSPs and fintechs should prepare for heightened diligence and upskilling.

The DGF must comply with the DPDP Act and should be consolidated with existing cyber security, IT, outsourcing and privacy frameworks rather than built as a standalone regime.

Model Behaviour: RBI Draws The Line on AI and Model Risk

BACKGROUND

On 24 June 2026, RBI released the Draft Guidance for public consultation. With growing reliance on models, driven by digitalisation, AI / ML adoption and third-party model providers, RBI cautioned that poorly managed models can lead to flawed decisions, financial losses, operational disruptions and compliance failures affecting REs, consumers and the financial system.

The Draft Guidance sets out principle-based expectations for model governance and risk management, calibrated to each RE's scale and the materiality of its models. It applies to all REs, SCBs (including foreign banks), SFBs, payments banks, LABs, RRBs, UCBs, RCBs, NBFCs across all four layers, AIFIs, asset reconstruction companies and credit information companies, and to all models, whether developed internally, sourced from third parties or a combination thereof. It is to be read with relevant RBI directions, which prevail in case of inconsistency.

ANALYSIS

Expansive definition of "model": A "model" is defined as any system that incorporates data, applies theoretical, empirical or judgement-based assumptions and statistical, mathematical, economic, financial or cognitive techniques (including AI / ML), and produces outputs used for business operations and decision-making. The definition captures algorithms, analytics, interfaces, applications and decision-based rules with a material impact on decision-making, regardless of whether the RE itself treats them as models.

Three lines of defence: REs must implement a three-lines-of-defence structure, with model owners as the first line, an independent model risk management and validation function as the second line, and internal audit as the third line.

Risk-based model tiering: All models must be classified under a risk-based tiering structure, reviewed at least annually, based on materiality, complexity and other relevant factors. The assigned tier drives validation prioritisation and intensity, approval routing (high-risk models re quire RMCB approval), risk mitigation, monitoring, inventory and documentation detail, and business continuity planning.

Model lifecycle management: Structured processes are prescribed across the model lifecycle, covering selection and development, independent validation (before and after deployment), approval (inc luding exceptions), ongoing monitoring, change management, and business continuity and decommissioning. REs must maintain a comprehensive inventory of all active, inactive and decommissioned models. Decommissioned models must be retained for at least ten years from decommissioning or the date they cease to serve as backup or benchmark reference, whichever is later, or such longer period as required under applicable law.

Third-party models: REs remain fully accountable for outcomes of third-party models, to which the MRMF applies mutatis mutandis. Such models are additionally subject to independent validation by the RE (notwithstanding any assurance from the third-party provider) and enhanced RMCB oversight irrespective of risk tier. Pre-acquisition due diligence and contractual safeguards covering access to technical documentation, audit rights and continuity/exit arrangements are required.

AI / ML-specific controls: AI / ML models attract additional requirements: defined explainability and transparency thresholds; safeguards against hallucinations (particularly for generative AI); fairness assessments to counter bias and discriminatory outputs; testing under adversarial and stressed scenarios; structured challenge such as red-teaming; controls for dynamic or automatic updates; and enhanced documentation for traceability, reproducibility and auditability. Deployment controls must address access controls, cyber risks and risks from external interfaces or APIs. Customer-facing systems must disclose that the user is interacting with an AI system and offer the option to switch to human assistance.

Human oversight: REs must establish human oversight for AI models, including human-in-command arrangements, override and kill-switch mechanisms, and periodic review of model outputs by personnel with adequate expertise.

Consumer protection: No model that harms consumers may be used. The RE's grievance-redressal mechanism must address grievances arising from consumer-facing models.

Key Takeaways

Governance uplift: REs will need to secure Board and RMCB oversight of model risk, adopt a formal risk-appetite statement, and set clear delegation structures, potentially requiring revisions to Board and committee charters.

Expanded scope of "model": The broad definition may bring within scope tools not previously treated as models. REs should conduct a gap analysis to identify, inventory, document and validate all tools that now qualify.

Vendor management: For third-party models, REs should review existing contracts for access to technical documentation, audit rights (for the RE and RBI), and continuity/exit arrangements. Procurement teams should build these requirements into new engagements.

AI / ML readiness: Institutions deploying generative AI, credit-decisioning algorithms and customer-facing chatbots will need dedicated investment in testing infrastructure, specialist personnel and documentation to meet explain-ability, red-teaming, bias-testing and human-oversight expectations.

Inventory burden: Maintaining a comprehensive inventory of all active, inactive and decommissioned models, with the prescribed retention periods, will demand significant data-management effort. REs should begin scoping their model landscape early.

04

SECURITIES AND INVESTMENT PLATFORMS

The past year has underscored that SEBI is no longer content with regulating traditional market intermediaries in isolation. Its gaze has expanded considerably to cover the technology layer that sits beneath and around the securities market: how data is governed, how AI models are deployed in decision making, how platforms advertise to retail investors, and how unregulated products like digital gold sit at the edges of the regulated ecosystem. The common thread is a regulator that recognises the securities market is now deeply intertwined with technology, and that effective oversight requires going beyond transaction level supervision to the governance of models, data, platforms and conduct.

On the AI front, SEBI has moved on two parallel tracks. One is defensive, responding to the growing threat of AI driven cyber vulnerabilities by mandating enhanced hygiene, patching, API security and coordinated monitoring through the Market SOC. The other is more forward looking, proposing a principle based framework for responsible AI and ML use in securities markets that covers model governance, explainability, fairness, testing and disclosure. The approach is measured: a tiered regime that distinguishes between customer facing uses (which attract higher compliance) and internal uses (which get a lighter touch), while making clear that responsibility cannot be outsourced regardless of who builds the model.

Equally notable is SEBI's push to clean up how the market communicates with investors. The proposed harmonised advertising framework replaces a scattered set of entity specific rules with a single code, bringing consistency across brokers, advisers, research analysts, mutual funds and bond platforms. The treatment of celebrity endorsements, the prohibition on dark patterns, and the shift from prior approval to post issuance reporting all point to a regulator trying to balance investor protection with operational practicality. SEBI's warning on digital gold fits the same pattern: where a product sits outside the regulatory perimeter but is marketed to retail investors, the regulator will not stay silent.

For market participants, the takeaway is that compliance is no longer limited to disclosures and capital adequacy. It now extends to how you build models, how you govern data, how you advertise, and how you manage the technology stack that powers your business. The firms that will thrive are those treating governance and risk management as a core operational capability rather than a periodic checkbox exercise.

Platform Reset: RBI Rewrites the Rules for Electronic Trading

BACKGROUND

An ETP is any electronic system, other than a recognised stock exchange, on which transactions in eligible instruments (securities, money market instruments, foreign exchange instruments, derivatives, etc.) are contracted, typically offering tailored tenures and faster settlement than an exchange.

RBI first regulated ETPs in 2018 through the Erstwhile ETP Directions. Driven by greater onshore-offshore forex integration, technological advancements, product diversity and market-maker requests to access offshore ETPs offering Indian Rupee (INR) products, RBI announced a review. Following the issue of the Draft Directions and stakeholder feedback, RBI issued the New ETP Directions on 16 June 2025, superseding the Erstwhile ETP Directions with immediate effect.

KEY AMENDMENTS

The New ETP Directions retain the 2018 regulatory architecture while recasting several provisions and adding new ones on enforcement, data governance and transitions. The key changes have been set out below.

Widened definition of "entity": The definition of "Entity" has been broadened from an incorporated company to "any person, whether natural or legal." Read with the outsourcing provisions, this brings outsourcing entities (which may not be incorporated companies) within the regulatory perimeter, without affecting the separate requirement that an ETP operator itself must be an incorporated company.

Eligibility criteria extended to banks: Under the Erstwhile ETP Directions, the general eligibility criteria did not apply to ETPs operated by (SCBs). The New ETP Directions remove this blanket exemption, so banks operating multi-dealer ETPs must now meet the same eligibility requirements as other operators, which include:

- Incorporation as a company in India
- The INR five crore minimum net-worth requirement
- The prescribed technological standards.

Strengthened experience requirement: While the Erstwhile ETP Directions required "its key managerial personnel" to have at least three years' experience in operating trading infrastructure, the New ETP Directions require a minimum of two key managerial personnel to hold such experience.

Recast single-dealer exemption: Previously, regulatory exemption extended to a bank running an ETP for its own customers on a bilateral basis, provided it did not give access to market makers and no real "market" was created. The New ETP Directions replace these vague conditions with a clearer carve-out for systems operated by SCBs (including branches of foreign banks in India) or SPDs that act as the sole quote/price provider and counterparty to all transactions. The carve-out requires such institutions to continue providing reports or information as required by RBI, which may still direct compliance or require authorisation in the public interest.

Transition to the PRAVAAH portal: The authorisation application process moves from physical submission to an electronic process through the RBI's PRAVAAH portal, enhancing accessibility, efficiency and real-time tracking for both applicants and the regulator.

New periodic reporting obligations: ETP Operators must now file

- A quarterly report on platform functioning, due by the 15th of the month following each quarter
- An annual compliance report, due by April 30 of the succeeding financial year. The first reports fell due by July 15, 2025 and April 30, 2026 respectively.

Enhanced data governance: Building on the existing obligation to preserve ETP data in easily retrievable media for at least 10 years, the New ETP Directions add that, on cancellation of authorisation or termination of operations, the operator must share all ETP data with RBI or any agency it specifies, in the form and manner directed, reinforcing post-termination accountability.

Outsourcing and risk management: Outsourcing arrangements are more clearly captured, with data-preservation, access and reporting obligations continuing to apply even after the arrangement ends. The risk-management framework is sharpened to require pre-trade and post-trade controls, and operators facilitating algorithmic trading must ensure that algo-system personnel are suitably skilled and that embedded model risks are managed.

Grandfathering: Any authorisation granted or action taken under the Erstwhile ETP Directions is deemed to have been granted or taken under the New ETP Directions. Existing operators therefore need not re-apply or seek fresh authorisation.

Offshore ETPs left unaddressed: Although a principal intent of the Draft Directions was to bring offshore ETPs (particularly those offering INR products to onshore participants) within the RBI's domain, the finalised New ETP Directions do not address this, leaving the treatment of offshore platforms an open question.

Key Takeaways

The New ETP Directions modernise RBI's oversight of trading infrastructure while preserving legal continuity for currently authorised operators.

The most consequential shift is for banks. By removing the blanket exemption for SCB-operated ETPs, RBI has levelled the playing field: banks running multi-dealer platforms must now meet the same incorporation, net-worth and technology standards as any other operator, potentially requiring public sector banks to house ETP operations in a separate corporate vehicle. Conversely, the single-dealer carve-out lets SCBs and SPDs run their platforms under a lighter compliance regime, though clients lose the competitive pricing of a multi-dealer venue, making transparency on pricing essential.

For all operators, the new quarterly and annual reporting requirements, together with strengthened data-preservation, data-sharing and risk-management obligations, raise the ongoing compliance burden, even as the PRAVAAH portal streamlines authorisation.

Finally, participants active on offshore INR platforms should note that this question remains unresolved and is likely to attract future regulatory attention.

All that Glitters: SEBI's Warning on Digital Gold

BACKGROUND

Digital gold products have gained significant traction in India, with several online platforms offering investors the ability to purchase fractional quantities of gold, marketed as a convenient alternative to physical gold. Major providers, along with their fintech distribution partners, facilitate online buying, selling and storage of gold, with the physical gold purportedly held in vaults on behalf of investors. However, these products are not issued or regulated under any securities or commodity derivatives legislation. Taking note of the growing adoption of such unregulated products, SEBI issued Press Release No. 70/2025 dated 8 November 2025, cautioning the public regarding the risks of dealing in digital gold / e-gold products.

ANALYSIS

Regulatory status of digital gold: SEBI has clarified that digital gold products are neither notified as "securities" under the SCRA nor regulated as "commodity derivatives". They therefore operate entirely outside SEBI's regulatory purview. This is in contrast to SEBI-regulated gold products, namely:

- Exchange-traded commodity derivative contracts
- Gold ETFs offered by mutual funds
- EGRs tradeable on stock exchanges, all of which can be accessed through SEBI-registered intermediaries and are governed by SEBI's prescribed regulatory framework

Investor risk warning: SEBI has flagged that digital gold products may entail significant risks for investors, including counterparty risk (i.e., the risk of default or failure by the platform or its underlying gold provider) and operational risk (i.e., risks arising from theft, data breaches or operational lapses). Critically, none of the investor protection mechanisms available under the securities market framework, including grievance redressal, are available to investors in digital gold products.

Key Takeaways

SEBI's press release signals a clear regulatory stance that digital gold, as currently structured, falls in a regulatory grey area with no statutory investor protections. While the press release does not amount to a ban, it serves as an unambiguous warning that investor recourse is limited. Market participants should monitor whether the regulatory framework evolves to bring digital gold within a formal regulatory structure, or whether further action follows this advisory.

Guard Rails and Kill Switches: SEBI takes on AI

BACKGROUND

SEBI issued its AI Advisory on 5 May 2026, which flags risks from emerging AI tools (such as Claude Mythos) that can identify and exploit system vulnerabilities at speed and scale. These risks relate to data confidentiality, application integrity and the reliability of outputs. SEBI has also formed a task force called cyber-suraksha.ai, comprising MIIs, QRTAs and other stakeholders, to coordinate on AI driven cyber risks. Given how closely market participants are interconnected, the AI Advisory requires SEBI REs to take a coordinated approach to vulnerability management, information sharing and monitoring, in line with SEBI's CSCRF.

Separately, SEBI issued its AI / ML Consultation Paper on 20 June 2025, proposing core guiding principles for the responsible use of AI and ML in securities markets. These principles remain proposals open for public comment and do not yet reflect SEBI's final position. The aim is to optimise the benefits of these technologies while safeguarding investor protection, market integrity and financial stability. SEBI notes that AI / ML usage has grown quickly due to greater data and computing power, along with advances in Gen AI and LLMs. Market participants currently use AI / ML mainly for advisory services, risk management, client monitoring, surveillance, pattern recognition, internal compliance and cyber security. The proposed principles would apply to Stock Exchanges, Clearing Corporations, Depositories, Intermediaries and Mutual Funds.

ANALYSIS

AI Advisory on Emerging AI Tools for Vulnerability Detection

Baseline Cyber Hygiene: The AI Advisory requires REs to:

- Apply the latest patches to all operating systems and applications immediately, using virtual patching where a permanent patch is not yet available
- Conduct regular vulnerability assessments, using AI based tools where possible, and security audits under the CSCRF
- Engage third party vendors to release and deploy timely patches, with exchanges and depositories directing their empanelled vendors to assess
- AI-led vulnerability risks and adopt safeguards such as VAPT, continuous monitoring and system hardening
- Follow structured change management, including documentation, impact analysis, review, testing and secure deployment, for any change to a system, however minor
- Harden their systems through secure configurations, removing unnecessary services and default accounts, and applying least privilege access and Zero Trust Network Access
- Periodically update their asset inventory and software bill of materials for critical applications, including open source components.

Monitoring, API Security and Governance: The AI Advisory requires REs to:

- Secure their APIs through a regularly updated inventory, strong authentication and authorisation on a least privilege basis, rate limiting, and whitelist based connections only
- Maintain day to day SOC monitoring that reviews even low priority alerts, supported by SOAR playbooks integrated with SIEM tools
- Expedite onboarding of eligible REs to the Market SOC (M-SOC) established by NSE and BSE, supported by MII awareness programmes
- Carry out periodic, scenario based risk assessments under the CSCRF, including of their third party providers, treating AI capability as a risk scenario
- Prepare, with guidance from their IT committees, a long term plan for using AI in detection and automated mitigation, recalibrating risk for AI accelerated threats

ANALYSIS: AI / ML CONSULTATION PAPER

Five Core Guiding Principles: The AI / ML Consultation Paper proposes five guiding principles for responsible AI / ML use, namely:

Model Governance

Model governance, calling for a skilled internal team, proper documentation, senior management oversight, independent audits, log retention, and periodic sharing of accuracy results and audit findings with SEBI

Fairness & Bias

Fairness and bias, requiring that models do not discriminate between customers, backed by controls to identify and remove bias from data sets

Investor Protection Disclosures

Investor protection and disclosure, requiring REs to disclose AI / ML usage that directly affects customers, covering the model's features, risks, limitations, accuracy, fees and data quality

Data Privacy & Cyber Security Measures

Data privacy and cyber security, requiring a clear policy, compliance with applicable laws, and reporting of technical glitches and breaches to SEBI. Responsibility for AI / ML services cannot be outsourced, so REs remain fully responsible for compliance even where such services are provided by third party vendors

Testing Framework

A testing framework, calling for testing in an environment separate from live systems, shadow testing using live data, retention of input and output data for at least five years, and continuous monitoring after deployment

Tiered, Lighter Touch Approach: A lighter compliance framework is proposed for AI / ML used for purposes other than business operations that directly affect customers. Internal use cases, such as compliance, surveillance and cyber security tools, would only need to meet a minimal set of principles, reducing the compliance burden for such uses.

Risk Based Control Measures: The AI / ML Consultation Paper also flags specific risks from AI / ML usage, together with proposed controls, signalling SEBI's likely future direction:

Malicious use leading to market manipulation or misinformation, such as fake statements or deepfakes, may be addressed through watermarking, provenance tracking, suspicious activity reporting and investor awareness campaigns

Concentration risk from reliance on a few Gen AI providers may be addressed by requiring REs to report vendor names, encouraging diversification, and subjecting dominant providers to enhanced monitoring as critical service providers

Herding and collusive behaviour may be addressed through diverse AI models and data sources, monitoring by stock exchanges, algorithmic audits and circuit breakers

A lack of explainability may be addressed through detailed process documentation, explainable AI requirements and human review of AI outputs

Model failure or runaway AI behaviour may be addressed through stress testing, circuit breakers, kill switches, and human oversight with accountability for AI driven decisions

Gaps in accountability and regulatory compliance may be addressed through regulatory sandboxes, human oversight and staff training on compliance risks.

Key Takeaways

The AI Advisory responds to emerging AI driven vulnerability detection tools by requiring REs to strengthen baseline cyber hygiene, secure APIs, expedite onboarding to the Market SOC, and build AI risk mitigation into their compliance obligations under the CSCRF.

Market participants using AI / ML in operations facing customers will need governance frameworks covering senior management oversight, documentation, independent audits and continuous monitoring across the model's lifecycle.

A tiered, lighter touch approach reduces the compliance burden for uses that do not face customers directly, such as internal compliance, surveillance and cyber security.

Responsibility for AI / ML services cannot be outsourced. REs will need to diligence vendors, put service level agreements in place, and maintain ongoing oversight.

Disclosure, testing, fairness, data quality and cyber security obligations will apply, along with periodic reporting to SEBI on accuracy results, audit findings, vendor names and breaches.

Risks from AI / ML use can be mitigated through measures such as watermarking, monitoring of vendor concentration, controls against herding, circuit breakers, explainability requirements, stress testing, kill switches, and regulatory sandboxes.

One Ad Code to Bind them: SEBI's Proposed Harmonised Advertising Framework

BACKGROUND

SEBI issued a Consultation Paper on a Common Advertisement Code for Specified SEBI Regulated Entities on 23 June 2026. Advertisement norms are currently governed through fragmented entity-specific regulations, master circulars and stock exchange circulars. While the proposals remain tentative, SEBI's intent is to consolidate these into a single harmonized framework in order to facilitate ease of doing business, investor protection, and regulatory consistency.

The Common Advertisement Code would apply to Stock Brokers, Depository Participants, IAs, RAs, OBPPs, Portfolio Managers and MFs including AMCs (together, "Specified SEBI RE"), and notably brings Depository Participants under a formal advertisement framework for the first time. A transition period of six months from notification is proposed.

ANALYSIS

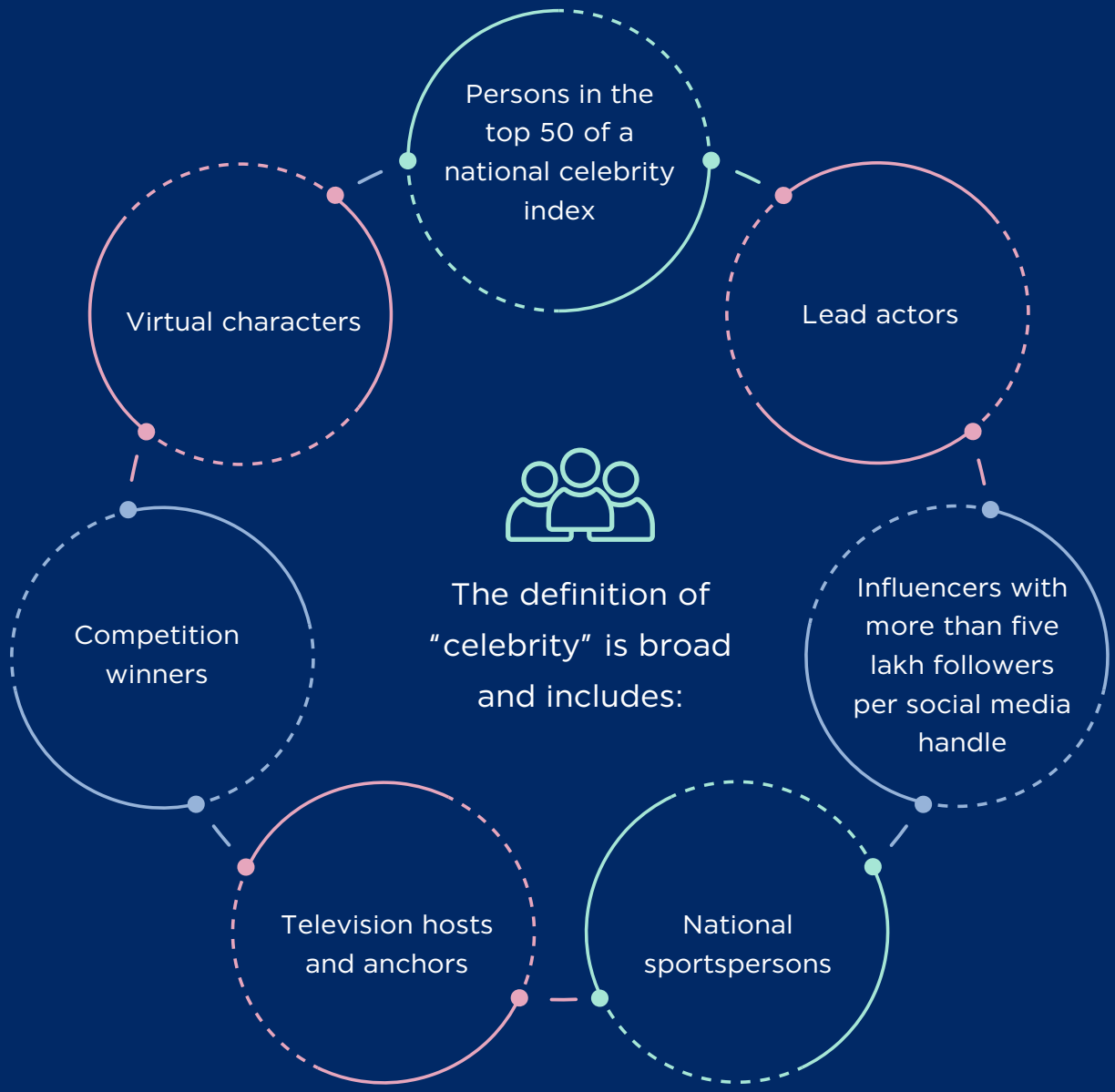
Comprehensive Definition of "Advertisement": "Advertisement" is defined widely to include any form of communication, endorsement or representation made through written, audio, visual, verbal or any other means, disseminated through any channel, including print, broadcast, digital and outdoor media, issued directly or indirectly by or on behalf of a Specified SEBI RE, that promotes or solicits any product, service, brand or entity. Most external-facing communications will fall within scope unless expressly carved out.

Excluded Communications: Certain communications are excluded from the definition of "advertisements", provided they carry no promotional or solicitation content. These include educational / informational material (subject to minimal branding, and reporting to the supervisory body where funded from education budgets), client reports and analyses, product or service lists, essential regulatory communications, responses to client queries, product demonstrations, greetings, recruitment communications, generic sponsorships, and client feedback surveys.

Shift from Prior Approval to Post-Issuance Reporting: Prior approval from exchanges (for stock brokers and OBPPs) and supervisory bodies (for IAs and RAs) would be replaced by post-issuance reporting model within 24 hours of issuance, except for celebrity endorsements, which continue to require prior approval. This is a material change for entities currently subject to prior approval, though mutual funds already operate on a post-issuance model.

Celebrity Endorsements Permitted at Brand Level Only

Celebrity endorsements would be permitted at the brand or entity level only, not for specific products or services. A promotion may list an RE's products / service but must carry no product-specific inducement or claim.



Celebrity advertisements require prior approval and prescribed disclaimers, and associated expenses of such celebrity advertisements cannot be passed on to investors or charged to a MF scheme.

Use of Ratings and Rankings only through PaRRVA: Ratings or rankings in advertisements may be used only if assigned by PaRRVA. Such ratings or rankings must be properly explained in the advertisement or through a link to the PaRRVA website or the website of the Specified SEBI RE, must be accompanied by a statement that they are only one factor to be considered, and must emanate from a study or survey covering all relevant market participants in the category to ensure comparability and objectivity.

Mandatory Disclosure Requirements: Every advertisement must disclose the entity's name, SEBI registration number and logo (if any), along with the prescribed disclaimers. For short-format content such as SMS, pop-ups and push notifications, where character limits make full disclosures impractical, a hyperlink to the full details on the entity's website may be used instead.

Supervisory Bodies identified for each RE Category: Relevant supervisory bodies for each category of Specified SEBI RE:

- Stock exchanges for stock brokers and OBPPs
- Depositories for depository participants
- The IAASB for IAs
- The RAASB for RAs
- AMFI for MFs and AMCs
- APMI for Portfolio Managers

Express Prohibition on Dark Patterns: Specified SEBI REs and their platforms must not engage in any dark pattern specified in Annexure I of the CCPA's Guidelines for Prevention and Regulation of Dark Patterns, 2023, such as false urgency, forced action and subscription traps.

General Obligations: Advertisements must be true, fair, accurate, complete and unambiguous, and must not be designed to mislead, disguise the significance of any statement, or exploit investors' lack of experience or knowledge. In particular, excessive technical or legal terminology must be avoided, and where specific securities / schemes are shown as examples, a prescribed disclaimer must accompany such examples. Statistical data, graphs and charts must disclose their source and relevant period. REs cannot offer incentives, vouchers or similar benefits to induce trading or onboarding or advertise during suspension. Where a third party issues an advertisement without an RE's consent, the RE must act within seven days, notify the supervisory body, and disclose the incident on its website.

Prohibited Content: Advertisements must not contain:

- False, misleading, exaggerated or ambiguous content or testimonials
- Any promise or assurance of guaranteed, risk-free or indicative returns
- Any promise of fixed returns (except for OBPPs or as specified);
- Content that disparages other regulated entities or makes unfair or imitative comparisons
- Misleading comparisons across products or asset classes of a different nature
- Content exploiting investor inexperience
- Logos or symbols of SEBI or MIIs unless permitted
- Content implying that past performance may recur
- References to past performance other than in the specified manner
- Indecent, vulgar or offensive content
- Anything otherwise prohibited under law

Post-issuance monitoring, enforcement and implementation: SEBI or the relevant supervisory bodies will conduct post-issuance monitoring, supported by a centralised digital reporting portal (with a common platform where multiple supervisory bodies apply) for advertisement uploads within 24 hours, and a separate system for approving celebrity advertisements. Non-compliance may lead to summary proceedings, withdrawal of advertisements, restraints on further advertising or onboarding of new clients, and monetary penalties.

Key Takeaways

The Common Advertisement Code replaces fragmented entity-specific and exchange-specific frameworks with a single harmonised code, benefiting entities registered in multiple regulated categories.

The shift to 24 hours post-issuance will require REs to build internal clearance, record-keeping and reporting workflows integrated with the new reporting portal. Only celebrity advertisements will continue to require prior approval.

Celebrity endorsements are permitted only at the brand or entity level, and not for specific products, and REs will be required to diligence their endorsers and structure advertisement campaigns accordingly.

Ratings and rankings may be used only where assigned by PaRRVA and only with prescribed explanatory disclosures.

Educational, factual and client-servicing communications without elements of product or service promotion are permitted. Short-format messaging may rely on a hyperlink to full disclosures.

The express prohibition on dark patterns will require entities and platforms to review their user interface and user experience design.

05

IFSCA

The IFSC GIFT City continues to carve out its position as India's gateway to global financial services, and IFSCA's regulatory output over the past year reflects a regulator that is moving with intent. Having laid the foundational payments framework in 2024, IFSCA has now turned its attention to two areas that will likely define the next phase of GIFT City's evolution: building the regulatory architecture for tokenization of real world assets, and consolidating the technology services ecosystem under a single, structured registration regime. Both signal a regulator that is keen to attract sophisticated global participants while maintaining credible guardrails.

On tokenization, the approach adopted is significant not just for what it proposes but for the posture it reflects. Rather than defaulting to prohibitions or waiting indefinitely, IFSCA has opted for a consultative, "same risk, same regulation" stance, seeking to accommodate DLT based market infrastructure within a familiar regulatory logic of issuance, custody, trading and settlement. The focus on real world assets (excluding crypto and CBDCs) keeps the scope grounded and commercially actionable for funds, bonds and financial products. On the technology services side, IFSCA has consolidated what was previously a circular driven, somewhat fragmented regime into a proper registration based framework with defined eligibility, fit and proper criteria, and governance expectations.

The broader trajectory is clear: IFSCA is positioning GIFT City not merely as an offshore booking centre but as a credible, innovation friendly jurisdiction that can compete with Singapore, Dubai and other established IFSCs for cross border financial services mandates. The reduced entry barriers, single window mechanisms and forward looking stance on digital assets are all consistent with this objective. For Fintech participants, the developments warrant close tracking, particularly as the tokenization framework moves from consultation to final policy and the registration timelines for technology services providers draw closer.

Digital Deeds: IFSCA Charts the Course for Asset Tokenisation

BACKGROUND

The IFSC GIFT City was established with the aim of making India a global leader in international financial services. IFSCA, the unified regulator for GIFT City, adopted a consultative approach in developing a regulatory framework for tokenization of real-world assets, constituting the Expert Committee on Asset Tokenization in September 2023 to recommend measures for developing a digital asset ecosystem. The resulting Consultation Paper, issued on 26 February 2025, defines tokenization as a process that uses new technologies to issue or represent assets in digital forms known as tokens, and is limited to real-world assets, whether tangible or intangible, excluding cryptocurrencies, crypto assets and central bank digital currencies.

Tokenization has the potential to transform how financial services operate, bringing transparency and traceability inherited from blockchain technology. Consequently, IFSCA highlights the need for regulating tokenization of certain RWAs, including financial securities (such as funds, bonds and stocks) and financial products (such as payments, deposits and bills receivable). IFSCA's opinions, approach, and the

intention of the proposed regulatory approach are presented across four question sets:

- Defining and characterizing digital tokens, including the rights they represent and how ownership is recognized.
- Evolving mechanisms for the issuance, custody, trading, clearing, and settlement of digital tokens.
- Evolving an appropriate risk management framework for digital tokens.
- Providing suitable catalysts for organic growth and development of the digital tokens market.

ANALYSIS

Defining and Characterizing Digital Tokens: Defining a digital asset or token varies across jurisdictions and regulators, depending on the purpose it serves. While a common classification is critical for legal, tax and regulatory certainty, this is a nuanced task given the varied characteristics and risks of different digital tokens. The type of underlying asset, whether real-world or native to a distributed ledger, affects the regulatory treatment. For tokens issued against real-world assets, key considerations include:

Whether the asset class is amenable to tokenization (having regard to behavioral characteristics, legal restrictions on ownership, public demand, and fungibility)

Creating a framework for the safe custody, upkeep and maintenance of the underlying asset

Ensuring legal and regulatory certainty when ownership changes as a result of token trades

Ensuring token holders have redemption or exit options at all times.

Rights Represented and Recognition of Ownership: The rights a digital token represent, commonly proportional ownership of the underlying asset or a beneficial interest in its revenues and must be clear to enable informed investment decisions. Equally important is how ownership is recognized: IFSCA distinguishes between bearer form, where holding the token itself confers ownership, and registered form, where ownership is recorded and given effect through a ledger maintained by the issuer.

Evolving Mechanisms for Issuance, Custody, Trading, Clearing and Settlement: Jurisdictions have not reached consensus on regulating tokenized assets, with the OECD noting that policymakers either apply existing financial regulations, introduce new tailor-made frameworks, or adapt existing rules to accommodate DLT. IFSCA and the Expert Committee have sought to envisage new architecture for the issuance, custody and secondary market transactions of digital tokens, and consider issuance (the minting of new tokens, with attendant risks of illegitimate or faulty issuance) and custody (safekeeping and management, whether self-custody or through a custodian) to be suitably regulated activities. In building a safe and reliable secondary market, IFSCA intends to apply the principle of "same risk, same regulation" so far as possible, while recognizing that DLT-based market infrastructure warrants differentiated treatment, considering:

The separation of trading, clearing and settlement functions

Changes to issuance and custody processes

Changes in the roles of market participants

The unique characteristics of distributed ledgers (such as whether they are public or private, and permissioned or permissionless)

Risk Management Framework: Given the rapid pace of evolution in tokenization, some jurisdictions have resorted to outright bans, which can stifle innovation and leave defrauded investors without recourse. IFSCA instead believes a comprehensive risk management framework can enable a regulated market, and has identified four focus areas:

Governance Risks

Arising from a wide range of use-cases coupled with lack of clarity on governance, notably the absence of adequate legal and regulatory controls, etc.

Technology Risks

Arising from heavy reliance on technology for performing functions previously performed by specialized entities, with operational vulnerabilities including scalability, uncertainty over settlement finality, and interoperability between different networks.

Cyber Risks

Arising from heavy reliance on cryptography and technology-enforced security.

ML / TF Risks

Arising from the cross-border nature of transactions, anonymity, regulatory arbitrage, differential privacy and KYC standards, etc.

Catalysts for Organic Growth: The challenges in the tokenization domain are being tackled by entities, industry associations and supra-national bodies through trial and error and constant innovation, requiring a balance between regulatory relaxation and safeguarding investor interests. IFSCA intends to minimize compliance burden, foster innovation and inspire public trust by:

Ensuring investor protection and awareness through suitable disclosures, due diligence requirements and grievance redressal mechanisms

Encouraging industry-wide best practices and standards to reduce compliance burden and accelerate innovation

Facilitating a lighter-touch regime through disclosure-based regulation and a sandbox approach

Key Takeaways

IFSCA is laying the groundwork for a first-of-its-kind regulatory framework for tokenized real-world assets, seeking to balance innovation with risk management, investor safeguards and public trust. The proposals remain at the consultation stage, and the final regulatory framework will depend on the responses received. Market participants should track IFSCA's eventual policy positions on token classification, ownership recognition, custody and settlement architecture, and DLT-specific regulatory treatment, as these will shape how tokenization of real-world assets operates in GIFT City.

From Circulars to Code: The Techfin and Ancillary Services Regulations

BACKGROUND

With the aim of providing a comprehensive regulatory framework for the technological ecosystem in IFSC GIFT City, IFSCA published the TechFin and Ancillary Services Regulations on 8 July 2025, consolidating the prior framework of two circulars, the Circular for Ancillary Services and the Circular for FinTech Entities, into a single registration-based regime.

The TechFin and Ancillary Services Regulations create a registration framework for TechFin and Ancillary Providers and set out the scope of financial services these providers may support, along with the permitted services and excluded activities. The regime was further expanded by the 2026 Amendment, which introduced a dedicated registration category for Trust and Company Services Providers.

ANALYSIS

Mandatory Registration Requirements: The TechFin and Ancillary Services Regulations outright prevent entities from commencing TechFin (i.e., technology solutions or services provided to aid, help, or assist in making arrangements for carrying on financial services) and/or Ancillary Services (i.e., services which aid, help, or assist in making arrangements for carrying on financial services) in the IFSC unless they receive a certificate of registration. Existing providers, authorized under the erstwhile circulars, must obtain the certificate of registration within 12 months of commencement

(i.e., by 8 July 2026). Until registered, such entities remain governed by the old framework.

Eligibility: The applicant must be a company or LLP in the IFSC, or a branch of a company or LLP incorporated outside the IFSC. The promoters or partners shall be from a jurisdiction which has not been identified in the FATF Public Statement.

The Registration Journey: The TechFin and Ancillary Services Regulations provide a streamlined procedure for the grant of certificate of registration.

The applicant shall apply via SWIT with the requisite documents and application fees.

On review, if the IFSCA is of the opinion that the certificate cannot be granted owing to deficiencies, it shall be communicated advising the applicant to rectify the same within 30 days. Failure to do so may result in rejection, subject to granting the applicant a reasonable opportunity of being heard via written submissions.

The IFSCA may grant in-principle approval, subject to conditions it deems fit.

Within 180 days of the same the applicant shall take steps to comply with the TechFin and Ancillary Services Regulations and the conditions.

The IFSCA may grant the certificate of rectification on satisfaction of compliance, subject to conditions it deems fit.

The certificate shall be valid unless suspended / cancelled by the IFSCA or voluntarily surrendered by the service provider.

Material changes shall be immediately furnished to the IFSCA.

Key Personnel: The TechFin and Ancillary Services Regulations require the appointment / designation of a Principal Officer, responsible for overall activities, and a Compliance Officer, responsible for the compliance of policies, procedures, record maintenance, and implementation of the TechFin and Ancillary Services Regulations and other applicable laws. They shall be full-time employees and based out of the IFSC.

Fit and Proper Requirements: The entity and its Principal Officer, Compliance Officer, directors / partners, and controlling shareholders must be "fit and proper" at all times, which entails financial integrity, good reputation, and honesty. The TechFin and Ancillary Services Regulations provide an extensive list of disqualifications, including conviction for an offence involving moral turpitude / economic offence, pending charge sheets / recovery proceedings, malfeasance, undischarged insolvency, unsound mind, willful defaulter status, and so on.

IFSCA's Powers: The IFSCA may:

Call upon for any information, documents, or records, which must be furnished

Require inspection of books of accounts, records, documents, infrastructure, procedures, and systems

Initiate any action it may deem fit in case of contravention of the TechFin and Ancillary Services Regulations and the circulars, guidelines, or direction issued thereunder

Introduction of Trust and Company Services Providers: The 2026 Amendment inserted a new chapter creating a distinct registration category for Trust and Company Services Providers (TCSPs), being TechFin and Ancillary Service Providers registered to provide trust and company services for leasing activities permitted by IFSCA. An entity wishing to offer TCSP services must obtain separate registration (even if it already holds a TechFin and Ancillary Services registration) and declare that it will maintain an arm's length relationship between its TCSP activities and its other services. Eligibility mirrors the general regime, i.e., incorporation as a company or LLP in the IFSC, with promoters or partners not from a jurisdiction identified in the FATF Public Statement. Permissible TCSP services (set out in the new Fifth Schedule) include acting as an agent for setting up trusts, companies or LLPs, acting as a trustee, director, company secretary, nominee shareholder or partner, and providing a registered office or business address.

Key Takeaways

The TechFin and Ancillary Services Regulations consolidate the erstwhile circular-based framework into a single registration regime, with defined eligibility, fit and proper, and governance standards for TechFin and Ancillary Service Providers. The Schedules define the regime's scope precisely, listing permitted Ancillary Services and TechFin Services, prohibited activities, and a Code of Conduct binding on all registered providers. The 2026 Amendment extends the regime to a new, separately registered category, TCSPs layering on bespoke governance, personnel, insurance and conflict of interest requirements reflecting the fiduciary nature of TCSP services.

GLOSSARY

2026 Amendment	International Financial Services Centres Authority (TechFin and Ancillary Services) (Amendment) Regulations, 2026
2FA	Two Factor Authentication
ACB	Audit Committee of the Board
Acquiring Bank	The bank which onboards the AePS touchpoint operators
AD Bank	Authorised Dealer Bank
AePS	Aadhaar Enabled Payment System, a payment system operated by NPCI that facilitates interoperable transactions using Aadhaar number and biometric or OTP authentication, enabling financial services such as cash withdrawal, cash deposit and fund transfer, and non-financial services such as mini statements and balance enquiry
AePS Directions	Reserve Bank of India – Aadhaar Enabled Payment System – Due Diligence of AePS Touchpoint Operators
AI	Artificial Intelligence
AI / ML Consultation Paper	Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets dated 20 June 2025
AI Advisory	Advisory on Emerging Advanced AI Tools for Vulnerability Detection (like Mythos) dated 5 May 2026
AIF	Alternative Investment Fund
AIFI	All India Financial Institutions
AMC	Asset Management Company
AMFI	Association of Mutual Funds in India
API	Application Programming Interface
APMI	Association of Portfolio Managers in India
ATO	AePS Touchpoint Operator, being the individual onboarded by the acquiring bank who operates the AePS touchpoint
BC	Business Correspondent
BCBS Data Principles	Basel Committee on Banking Supervision Principles for Effective Risk Data Aggregation and Risk Reporting
BINs	Bank Identification Numbers
Board	Board of Directors
BR Act	Banking Regulation Act, 1949
CCD	Compulsorily Convertible Debenture
CCPA	Central Consumer Protection Authority
CDD	Customer Due Diligence
CERT-IN	Computer Emergency Response Team
CGM	Chief General Manager
Circular for Ancillary Services	Circular dated 10 February 2021, "Framework for enabling Ancillary services at International Financial Services Centres"
Circular for FinTech Entities	Circular dated 27 April 2022, "Framework for FinTech Entity in the International Financial Services Centres"
CKYCR	Central KYC Records Registry

CME Amendment Directions	Reserve Bank of India (Commercial Banks – Credit Facilities) Amendment Directions, 2026 (Revised) dated 30 March 2026
CMI	Capital Market Intermediary
CNP	Card not present
CoA	Certificate of Authorisation
Common Advertisement Code	Common Advertisement Code for Specified SEBI Regulated Entities dated 23 June 2026
Companies Act	Companies Act, 2013
Consultation Paper (Advertising)	Consultation Paper on Common Advertisement Code for Specified SEBI Regulated Entities
CPV	Contact Point Verification
CRM	Credit Risk Management
CRM Amendment Directions	Reserve Bank of India (Credit Risk Management) – Amendment Directions, 2026 dated 5 Ja ary 2026
CRM Directions	Reserve Bank of India (Credit Risk Management) Directions, 2025 dated 28 November 2025
CSCRF	SEBI's Cyber Se curity and Cyber Resilience Framework
Cyber Resilience Master Directions	Reserve Bank of India – Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators
DGC	Data Governance Committee
DGF	Data Governance Framework
Digital Payment Authentication Directions	Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025
DLT	Distributed Ledger Technology
DMA	Direct Marketing Agent
DoT	Department of Telecommunications
DPDP Act	Digital Personal Data Protection Act, 2023
Draft Data Governance Guidance	Reserve Bank of India Draft Guidance on Regulatory Expectations for Data Governance
Draft Directions	Draft Master Direction – Reserve Bank of India (Electronic Trading Platforms) Directions, 2024, placed for public comments on 29 April 2024
Draft MRMF	Draft Guidance on Regulatory Principles for Model Risk Management
Draft PPI Directions	Draft Reserve Bank of India (Prepaid Payment Instruments) Directions, 2026
DSA	Direct Selling Agent
EGR	Electronic Gold Receipts
Erstwhile ETP Directions	Electronic Trading Platforms (Reserve Bank) Directions, 2018
ETF	Exchange Traded Fund
ETP	Electronic Trading Platform
Expert Committee	Expert Committee on Asset Tokenization
FATF	Financial Action Task Force
FATF Public Statement	Financial Action Task Force public statement "High-Risk Jurisdiction subject to call for action"
FEMA	Foreign Exchange Management Act, 1999

First SBR Amendment Directions	Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Amendment Directions, 2026 dated 29 April 2026
FIU-IND	Financial Intelligence Unit – India
Gen AI	Generative Artificial Intelligence
HFC	Housing Finance Companies
IA	Investment Adviser
IAASB	Investment Advisers Administration and Supervisory Body
IFSC GIFT City	International Financial Services Centre, Gujarat International Finance Tec-City
IFSCA	International Financial Services Centres Authority
IFSCA Consultation Paper	International Financial Services Centres Authority Consultation Paper dated February 26, 2025 "Regulatory Approach Towards Tokenization of Real-World Assets"
InCA	Inward Collection Account
INR	Indian Rupees
InvITs	Infrastructure Investment Trusts
IRDAI	Insurance Regulatory and Development Authority of India
IS	Information Security
IT	Information Technology
JV	Joint Venture
KFS	Key Facts Statement
KMP	Key Managerial Personnel
KYC	Know Your Customer
LAB	Local Area Banks
LLMs	Large Language Models
LLP	Limited Liability Partnership
LSP	Lending Service Provider
M-SOC	Market Security Operations Centre established by NSE and BSE
MDR	Merchant Discount Rate
MF	Mutual Fund
MII	Market Infrastructure Institution
MITC	Most Important Terms and Conditions
ML	Machine Learning
NBFC	Non-Banking Financial Companies
NBFC-UL	NBFCs in the Upper Layer
NETC	National Electronic Toll Collection
New ETP Directions	Master Direction – Reserve Bank of India (Electronic Trading Platforms) Directions, 2025, Notification No. FMRD.MIOD.03/14.03.027/2025-26 dated 16 June 2025
NOC	No Objection Certificate
NOFHC	Non-Operative Financial Holding Companies

NOFHC Amendment	Reserve Bank of India (Non-Operative Financial Holding Company) (Amendment) Directions, 2025 dated 5 December 2025
NOFHC Directions	Reserve Bank of India (Non-Operative Financial Holding Company) Directions, 2025 dated 28 November 2025
NPCI	National Payments Corporation of India
NRI	Non-Resident Indian
OBPP	Online Bond Platform Provider
OCA	Outward Collection Account
ODR	Online Dispute Resolution
OTP	One Time Password
OVD	Officially Valid Document
P2P	Person to Person
PA	Payment Aggregator
PA Directions	Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025
PA-CB	Payment Aggregator – Cross Border
PA-O	Payment Aggregator – Online
PA-P	Payment Aggregator – Physical
PaRRVA	Past Risk and Return Verification Agency
PCI-DSS	Payment Card Industry Data Security Standard
PCI-SSF	Payment Card Industry Software Security Framework
PFRDA	Pension Fund Regulatory and Development Authority
PG	Payment Gateway
PIN	Personal Identification Number
PPI	Prepaid Payment Instrument
PPI MD	Master Directions on Prepaid Payment Instruments dated 27 August 2021
PPI-MTS	Prepaid Payment Instrument – Mass Transit Systems
PSO Outsourcing Framework	Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators
PSP	Payment System Provider
PSS Act	Payment and Settlement Systems Act, 2007
QRE	Qualified Regulated Entity
QRTA	Qualified Registrar to an Issue and Share Transfer Agent
RA	Research Analyst
RAASB	Research Analysts Administration and Supervisory Body
RBI	Reserve Bank of India
RBI Act	Reserve Bank of India Act, 1934
RCB	Rural Co-operative Banks
RE	An entity regulated by RBI, SEBI or another financial sector regulator. The specific categories of REs covered vary by writeup; see the applicability section of each writeup.

REITs	Real Estate Investment Trusts
Responsible Business Conduct Amendment Directions	Reserve Bank of India (Responsible Business Conduct) Second Amendment Directions, 2026
Responsible Business Conduct Directions	Reserve Bank of India (Responsible Business Conduct) Directions, 2025
RMCB	Risk Management Committee of the Board
RRB	Regional Rural Banks
RWA	Real-World Asset
SBR Directions	Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025 dated 28 November 2025
SCB	Scheduled Commercial Bank
SCB Credit Directions	Reserve Bank of India (Commercial Banks – Credit Facilities) Directions, 2025 dated 28 November 2025
SCRA	Securities Contracts (Regulation) Act, 1956
SEBI	Securities and Exchange Board of India
SEBI RE	SEBI Regulated Entity
Second SBR Amendment Directions	Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Second Amendment Directions, 2026 dated 24 June 2026
SFB	Small Finance Banks
SIEM	Security Incident and Event Management
SMS	Short Messaging Service
SOAR	Security Orchestration and Automated Response
SOC	Security Operations Centre
SPD	Standalone Primary Dealer
Specified Regulated Entities	Stock Brokers, Depository Participants, Investment Advisers, Research Analysts, Online Bond Platform Providers, Portfolio Managers and Mutual Funds including Asset Management Companies
SPV	Special Purpose Vehicle
SSOT	Single Source of Truth
SWIT	Single Window IT Systems
TAT	Turn Around Time
TCCCPR	Telecom Commercial Communication Customer Preference Regulation, 2018
TCSP	Trust and Company Services Provider
TechFin and Ancillary Services Regulations	International Financial Services Centres Authority (TechFin and Ancillary Services) Regulations, 2025
Third SCB Credit Amendment Directions	Reserve Bank of India (Commercial Banks – Credit Facilities) Third Amendment Directions, 2026 dated 10 June 2026
TPPS	Third-party product or service
TPPSP	Third-Party Product or Service Provider
TRAI	Telecom Regulatory Authority of India

UCB	Urban Co-operative Banks
UFS Second Amendment Directions	Reserve Bank of India (Non-Banking Financial Companies – Undertaking of Financial Services) Second Amendment Directions, 2026
UFS Directions	Reserve Bank of India (Non-Banking Financial Companies – Undertaking of Financial Services) Directions, 2025
UPI	Unified Payments Interface
V-CIP	Video-based Customer Identification Process
VAPT	Vulnerability Assessment and Penetration Testing
ZTNA	Zero Trust Network Access

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with 1300+ legal professionals, including 340+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com

Contributors

Smita Jha
Partner
Banking & Finance
smita.jha@khaitanco.com

Prashanth Ramdas
Partner
Banking & Finance
prashanth.ramdas@khaitanco.com

Diksha Singh
Principal Associate
Banking & Finance
diksha.singh@khaitanco.com

Akshay Ferdinand
Senior Associate
Banking & Finance
akshay.ferdinand@khaitanco.com

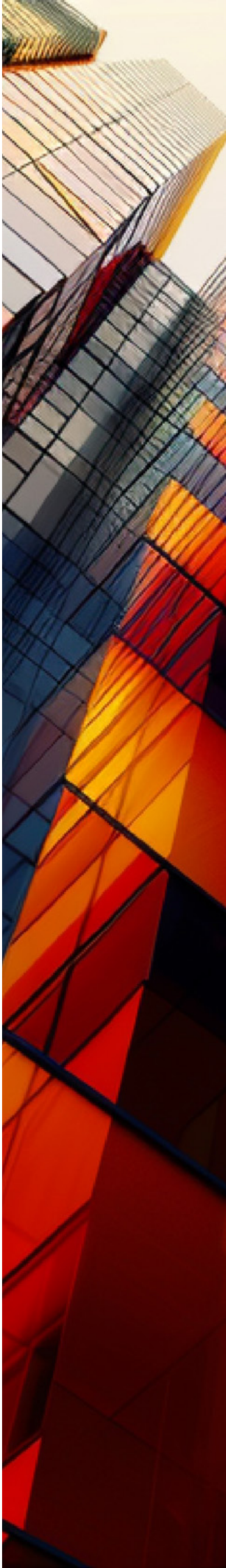
Viti Bansal
Associate
Banking & Finance
viti.bansal@khaitanco.com

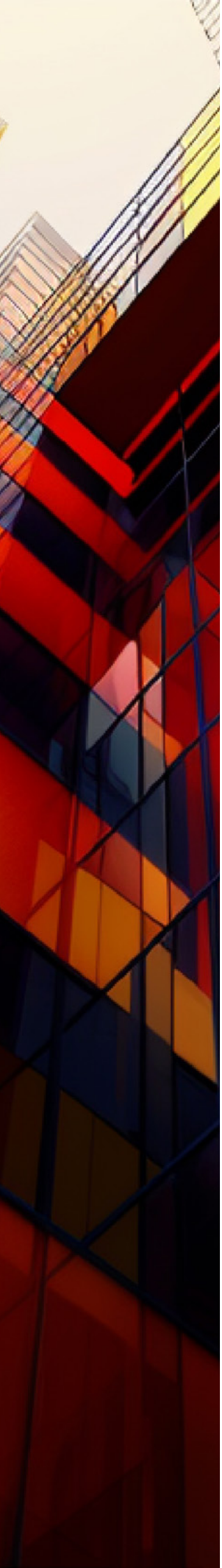
Chaitra T Bhat
Associate
Banking & Finance
chaitra.bhat@khaitanco.com

Aishwarya Alla
Associate
Banking & Finance
aishwarya.alla@khaitanco.com

Anisha Chakrabarti
Associate
Banking & Finance
anisha.chakrabarti@khaitanco.com

Sameep Baral
Associate
Banking & Finance
sameep.baral@khaitanco.com





About Unified Fintech Forum

The Unified Fintech Forum (Formerly, DLAI) stands as a pivotal entity in India's rapidly evolving financial technology landscape, serving as a non-profit advocacy organisation dedicated to fostering collaboration, innovation, and responsible growth within the fintech sector. Functioning as a unified voice for the diverse array of fintech companies operating in India, the forum plays a crucial role in shaping the regulatory environment, promoting best practices, and driving financial inclusion across the nation. By bringing together startups, established financial institutions, technology providers, and policymakers, the Unified Fintech Forum creates a collaborative ecosystem where ideas can be exchanged, challenges can be addressed collectively, and the transformative potential of fintech can be harnessed for the benefit of all stakeholders. The forum's activities encompass a wide range of initiatives, including advocacy efforts to aid in policy making, capability and capacity building programs in fintech domain to enhance awareness and understanding of fintech, research reports to provide insights into market trends, and networking events to facilitate connections and partnerships within the industry. Through these activities, the Unified Fintech Forum strives to create a conducive environment for fintech innovation, ensuring that India remains at the forefront of the global fintech revolution. The organization acts as a bridge between regulators, policymakers, investors and fintech companies, offering suggestions and innovative solutions to the stakeholders. It is becoming a significant focal point for everyone involved in the financial services industry of India.

To know more, visit www.unifiedfintech.in