jsa
advocates & solicitors

Knowledge Management

Semi-Annual FinTech Compendium 2025

July – December 2025

Semi-Annual FinTech Compendium 2025

Introduction

This Compendium consolidates all the key developments undertaken in the FinTech sector in India which were circulated as JSA Newsletters/Prisms during the calendar period from July 2025 till December 2025.

Reserve Bank of India

Balancing innovation and risk: How India's financial regulators are approaching Artificial Intelligence

On August 13, 2025, the Reserve Bank of India ("**RBI**") released the Framework for Responsible and Ethical Enablement of Artificial Intelligence ("**FREE-AI**") Committee Report ("**FREE AI Report**"). This marks a step towards India's approach to Artificial Intelligence ("**AI**") governance. The FREE AI Report lays the foundational principles of responsible and ethical adoption of AI in the banking sector.

The Ministry of Electronics and Information Technology ("**MeitY**"), alongside the sectoral regulators such as RBI and the Securities and Exchange Board of India ("**SEBI**"), have been wary of the increasing adoption and integration of AI and Machine Learning ("**ML**") across sectors, particularly in the financial product or services sector. Starting with the Government's policy wing, NITI Aayog, publishing a series of policy papers on responsible AI principles back in 2018, India has witnessed several policy initiatives by way of sector specific guidance and sub-committee reports aiming to regulate AI. However, these guidance continue to remain non-binding and advisory in nature.

Free AI Report

In December 2024, RBI unveiled its plans to constitute a FREE-AI committee to provide recommendations to develop an AI regulatory framework in the financial and banking sector. This committee was tasked with coming up with guardrails that enable innovation as well as mitigate risk.

The FREE AI Report identifies AI as a transformative technology reshaping financial services, offering both significant opportunities such as increased inclusion and heightened efficiency, and notable risks like bias, opacity, and cybersecurity threats. The FREE AI Report highlights the increasing integration of AI and ML in financial sector applications, from credit assessment and fraud detection to customer service improvements and recognises the need for a responsible and ethical framework for AI adoption by India's diverse and evolving financial ecosystem.

The FREE AI Report's approach is underpinned by the following 7 (seven) fundamental 'Sutras' (guiding principles):

1. trust as the foundation;
2. people first;
3. innovation over restraint;
4. fairness and equity;
5. accountability;
6. understandable by design, and safety; and
7. resilience and sustainability.

These principles are designed to ensure that AI adoption in finance enhances public trust, supports human judgment, promotes inclusion and fairness, and is auditable, explainable, and robust. The FREE-AI committee stresses the importance of fostering both innovation and effective risk mitigation and operationalises the 'Sutras' into 2 (two) complementary sub-frameworks:

1. **Innovation Enablement' framework**: This framework focuses on strengthening the sector's infrastructure (shared data and compute resources, sandboxes), adopting agile and adaptive policies, and building institutional and human capacity for AI innovation. It lays down recommendations for enabling innovation under 3 (three) pillars: infrastructure; policy; and capacity. The recommendations include establishing a high-quality financial sector data infrastructure; launching AI innovation sandboxes; supporting indigenous financial sector-specific AI models; integrating AI with digital public infrastructure; developing adaptive, principle-based regulatory policies; and incentivising AI-driven affirmative actions for financial inclusion.
2. **'Risk Mitigation' framework**: This framework mandates robust governance, consumer protection, continuous assurance, and focused oversight over the deployment and operations of AI systems in financial services. It also lays down recommendations for risk mitigation under its own 3 (three) pillars: governance; protection; and assurance. On the risk mitigation front, the FREE AI Report prescribes board-approved AI policies, comprehensive data governance, structured model validation, mandatory red teaming (an adversarial testing approach designed to challenge AI systems to reveal hidden vulnerabilities, stress points, and risks) of high-risk AI, robust business continuity plans, AI incident reporting, comprehensive AI audit frameworks, transparent public disclosures, and standardised compliance toolkits to ensure responsible and trustworthy AI adoption across institutions.

Under these 2 (two) frameworks, the FREE-AI Report provides 26 (twenty-six) recommendations to operationalise the proposed regulatory framework for AI governance in the financial sector.

SEBI's approach to AI governance in financial market

Alongside RBI, SEBI has also been on the frontier of AI governance in the Indian financial market. The increasing adoption of AI/ML technologies across financial markets in areas such as risk management, surveillance, compliance, and advisory services within stock exchanges, brokers, and mutual funds, has prompted SEBI to consider the risks and benefits posed by such AI systems. In this regard, SEBI released a consultation paper on June 20, 2025, on the proposed guidelines for the responsible usage of AI and machine learning in securities market and sought public and

stakeholder comments. SEBI has put together recommendations to safeguard investor protection, ensure market integrity, and maintain financial stability in the Indian financial market.

The key recommendations set out in the consultation paper focus on establishing stringent model governance practices, robust testing frameworks, ongoing monitoring, and clear accountability for AI/ML implementations. The principles outlined require market participants to set up skilled internal teams, engage in continuous risk assessment, maintain comprehensive documentation, and adopt fallback mechanisms for model failures.

The consultation paper further emphasises on enhanced disclosure requirements to clients, anti-bias controls, independent auditing, periodic accuracy reporting to SEBI, and strict data privacy and cybersecurity measures. The proposal introduces a tiered regulatory approach, offering a light-touch regime for AI/ML systems not directly impacting clients, such as those used exclusively for internal compliance or surveillance.

Additionally, in February, SEBI notified an amendment to the SEBI (Intermediaries) Regulations, 2008 which introduced a new chapter relating to usage of AI. Per the amendment, persons and entities regulated by SEBI using AI/ML tools whether developed in-house or sourced from third parties are solely responsible for the privacy, security, and integrity of investors' and stakeholders' data, including fiduciary data, throughout all processes. They are also fully accountable for any outputs generated by such tools and for ensuring compliance with all applicable laws.

Code for Regulated Entities – developments in other jurisdictions

Several jurisdictions and their regulators are also introducing their own self-regulatory and guidance-based approaches to regulate AI adoption in financial services.

Financial regulators such as Monetary Authority of Singapore ("**MAS**") in Singapore issued guiding principles for the use of AI and data analytics in the financial sector. The MAS has issued sector-specific 'FEAT' principles (Fairness, Ethics, Accountability, and Transparency) for the financial services market. While these guidelines are not mandatory, they aim to guide banks, insurance companies, capital market intermediaries, and other entities supervised by MAS.

Similarly, United Kingdom's financial regulator, the Financial Conduct Authority, and the Bank of England published a joint discussion paper (DP5/22) on 'Artificial Intelligence and Machine Learning' in the financial sector. The paper examined the unique risks and challenges posed by AI/ML, including issues related to governance, model accountability, transparency, and regulatory gaps and suggested guiding principles to be adopted by financial market players.

Further, the European Union's AI Act ("**AI Act**") became the first binding law (will come to effect in a phased manner) to govern AI systems, however, it does not contemplate sectoral approach but rather an approach based on the risk which the AI tool poses. Further, the European Commission also released 'General Purpose AI Code of Practice' as a voluntary tool for the general-purpose AI models (one trained on large-scale data using self-supervision, capable of performing a wide range of tasks, and adaptable for integration into various systems, such as ChatGPT) to comply with the legal obligations on safety, transparency and copyright under the AI Act.

Conclusion

The FREE AI Report suggests AI-specific enhancements to existing RBI master directions. For instance, in the directions governing outsourcing of functions under Regulated Entities ("**REs**"), a suggested enhancement is to incorporate obligations to disclose the use of AI by third-party vendors and their subcontractors. Similarly, under the cyber security frameworks in

banks, capturing AI specific threats such as model poisoning and adversarial attacks in the risk assessments under cyber security policy and establish protocols for monitoring and mitigating AI related cybersecurity incidents. By providing both a principled foundation and actionable recommendations, the framework seeks to balance innovation with robust governance, making responsible AI adoption in the financial sector.

AI presents India with an opportunity to accelerate growth, improve governance, and solve challenges at scale. To unlock this potential, India must adopt a forward-looking regulatory approach. One that nurtures innovation, ensures accountability, and builds public trust. Striking this balance will be key to shaping an AI ecosystem that not only drives development but also safeguards our collective future.

Know Your Customer

With an aim to enhance financial inclusion while ensuring robust Customer Due Diligence ("**CDD**"), RBI, on August 14, 2025, amended the Know Your Customer ("**KYC**") Master Direction, 2016 ("**KYC MD 2016**"). The amendments strengthen customer onboarding, clarify the scope of obligations for REs, and introduce safeguards for Persons with Disabilities ("**PwDs**").

The revised KYC MD 2016 requires REs to adopt customer acceptance policies that do not result in denial of services to PwDs, and to ensure that applications for onboarding or KYC updation are not rejected without due consideration, with reasons for rejection duly recorded. REs may now also rely on third-party due diligence not only at the commencement of account-based relationships, but also for occasional high-value transactions and international money transfer operations.

Further, the amendments expand biometric-based e-KYC to include Aadhaar face authentication, which may be conducted through bank staff or authorised agents. Importantly, the liveness check in the video-based customer identification process must be implemented in a manner that does not exclude persons with special needs.

Subsequently, RBI, on November 28, 2025, issued new Master Directions on KYC, namely the consolidated RBI (Commercial Banks - KYC) Directions, 2025 ("**KYC MD 2025**"). This consolidation is part of RBI's broader regulatory review exercise aimed at reducing compliance complexity by organising instructions separately for each class of RE.

The primary intent was to consolidate the plethora of existing circulars and the KYC MD 2016 into a single, comprehensive document on an 'as-is' basis, removing obsolete instructions and improving clarity without introducing major substantive changes to the core KYC obligations.

While RBI invited stakeholder comments on the draft versions to ensure completeness and accuracy, the final text largely retains the existing framework, barring minor editorial re-organisations and the inclusion of specific explanations or provisos to address ambiguities (listed in the table below).

The new structure

Notably, while the new KYC MD 2025 is explicitly titled for 'Commercial Banks', it has immediate legal implications for Payment System Providers ("**PSPs**"), including Prepaid Payment Instrument ("**PPI**") issuers and Payment Aggregators ("**PAs**"). Concurrently with this issuance, RBI released a specific notification repealing the KYC MD 2016. Consequently, the notification mandates that all references to the KYC MD 2016 in existing payment system instructions (such as the Master Directions on PPIs and PAs) must now be read as references to the new KYC MD 2025. Therefore, despite the nomenclature, the compliance teams must map their KYC protocols to the specific paragraphs of the new KYC MD 2025.

A high-level summary of the structural shifts and relevant updates is provided in the table below:

Clause under the KYC MD 2025	Original clause	Change made
KYC Identifier definition (Clause 5(xii))	KYC Identifier was previously defined as the unique number or code assigned to a customer by the Central KYC Records Registry ("**CKYCR**"). It contained no explanation to explain how a customer can obtain their KYC Identifier.	An explanation is added to the definition stating the following: A customer can obtain his KYC Identifier through the following way: during the account opening process, once the customer's KYC Identifier is generated by CKYCR and provided to the bank, the bank will share the same with the concerned customer; and the customer has the option to access his KYC Identifier on CKYCR portal at www.ckycindia.in.
KYC policy (Clause 6(4)(i))	The KYC MD 2016 discussed due diligence measures to deal with requests by customers to change registered mobile numbers for non-face-to-face accounts. However, this requirement was only mentioned in the specific section on opening accounts via Aadhaar One-Time Password ("**OTP**") in clause 17(ii), not as a mandatory element of the high-level board policy.	The KYC MD, 2025 requires the board-approved KYC policy to include a robust due diligence process for dealing with requests to change registered mobile numbers for non-face-to-face accounts.
CDD procedure in case of individuals (Clause 23)	If the customer has a KYC Identifier, the RE must fetch their KYC records from CKYCR. If e-KYC cannot be done due to illness, injury, old age or similar reasons, the RE must take the Aadhaar number and verify the customer through offline verification or another Officially Valid Documents ("**OVDs**"), and record this as an exception in a centralised, auditable database. Aadhaar numbers must be redacted when authentication is not required. Biometric e-KYC can be done by authorised bank officials or business correspondents, and all Aadhaar users must comply with the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 ("**Aadhaar Act**").	Explanation 4 is added stating the following: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act, the customer will provide the Aadhaar number to the bank. In other cases, customers may provide the Aadhaar number voluntarily.
V-CIP infrastructure (Clause 27(1)(v))	The V-CIP infrastructure will have components with face liveness/spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the bank.	An explanation is added stating the following: Making specific facial gestures, such as blinking of eyes, smiling, frowning, is not mandatory for liveness check. The bank will take due cognisance of special needs, if any, of the customer during liveness check.

Clause under the KYC MD 2025	Original clause	Change made
Conditions for small accounts (proviso to Clause 28(4)(ix))	The conditions for small accounts require a self-attested photograph and certification by a bank officer (or the jail officer, for prisoners), confirming the customer signed or affixed a thumbprint in their presence. These accounts may be opened only at core banking solution linked or manually monitored branches, and banks must ensure monthly and annual transaction and balance limits are not exceeded. They operate for 12 months, extendable by another 12 months if the customer shows proof of having applied for an OVD. All relaxations are reviewed after 24 months. Small accounts remain operational during Government-notified periods and must be monitored for suspicious activity, in which case full KYC is required. Foreign remittances cannot be credited unless the customer's full KYC is completed.	A proviso is added stating the following: If the bank renders any account ineligible for being classified as a small account due to credits/balance in the account exceeding the permissible limits, the bank may allow withdrawals within the limit prescribed for small accounts where the limits thereof have not been breached.

Conclusion

While the KYC MD 2025 largely preserves the 'as-is' framework of the previous regulations, it signals a shift toward a more organised and distinct regulatory architecture. For PAs and PSPs, the immediate challenge is administrative rather than structural; accurately mapping internal protocols to the new 'Commercial Bank' standards to replace the now-repealed KYC MD 2016. By proactively addressing the specific nuances, ranging from V-CIP accessibility to KYC identifier handling, compliance teams can ensure a seamless transition that aligns with RBI's ultimate goal of reducing compliance complexity.

Legal and regulatory analysis of RBI's Master Direction on PAs

RBI has released the new Master Directions on the Regulation of PAs, effective September 15, 2025 ("**New PA Directions**"). This move, which follows public consultations on draft PA amendments released in April 2024 ("**Draft PA Amendments**"), aims to rationalise regulations and bring more clarity to the sector. The New PA Directions supersede previous guidelines ("**2020 PA Directions**"), including those for Online PAs ("**PA-O**") and Cross-Border PAs ("**PA-CB**").

PA categories and definitions

1. **New provision**: The distinction between different types of PAs has been formalised. The New PA Directions introduce the following 3 (three) distinct categories of PAs, aiming to bring all modes of payment aggregation under a single regulatory umbrella.
   a) PA-Physical ("**PA-P**"): A PA that facilitates transactions where both the payment acceptance device and the payment instrument are physically present and in close proximity.
   b) PA-O: A PA that facilitates transactions where the acceptance device and payment instrument are not in close proximity.
2. **PA-CB**: A PA that facilitates aggregation of cross-border payments for current account transactions for its onboarded merchants.
3. **What has changed**: The Draft PA Amendments first introduced the concepts of PA-P and PA-O to extend PA regulation to offline payments. The New PA Directions elaborate on this by clarifying that the 'acceptance device' and 'instrument' must be in close proximity for a transaction to be classified as physical. The definitions of PA-CB have also been clarified, with specific exclusions for AD Category-

II non-banks and card network-settled transactions.

4. **Practical implication**: While this distinction clarifies the regulatory scope, it introduces a grey area in the context of mobile-based payments like Unified Payment Interface ("**UPI**") QR codes. For instance, a QR code displayed on a phone in a physical store would likely be considered a PA-P transaction, as the acceptance device (the merchant's phone) and the instrument (the customer's phone) are in close proximity. However, an SMS link with a QR code sent to a customer's phone for payment later could be considered a PA-O transaction, as the proximity element is absent. The New PA Directions do not provide specific guidance on such hybrid use cases, leaving some room for interpretation.

Authorisation and capital requirements

1. **New provision**: All non-bank entities are required to apply for authorisation as a PA. For PAs who already have a Certificate of Authorisation ("**COA**"), must intimate RBI the following:

   a) if the entity is already conducting PA-P business, it must formally intimate RBI. The timeline for such intimation is not specified; and

   b) if the entity wishes to start a new type of PA business (e.g., PA-O or PA-CB), then it must intimate RBI at least 30 (thirty) days before commencing the new business. If an entity's application for a PA-O or PA-CB COA is currently under consideration by RBI, it must inform RBI about any existing PA-P business. This intimation must be done through the online portal by December 31, 2025.

2. **Specifics for entities only in PA-P business**: If the entity only performs PA-P business, it must apply for COA as a PA by December 31, 2025. Failure to apply by this deadline will result in a mandatory winding up of business. The entity must immediately inform its banker(s) and cease all business operations by February 28, 2026.

3. **Practical implication**: The lack of a specific timeline for existing PAs with a COA to intimate RBI about their PA-P business could be a point of ambiguity, although the broader deadline of December 31, 2025, for authorisation applications likely applies. This move brings all PA activities, including physical payments, under a regulated and consistent capital framework.

Third-party payouts

1. **New provision**: A PA is permitted to make a payment to a third party at the specific direction of a merchant. This is only allowed if 2 (two) conditions are met:

   a) the merchant has a physical or online presence with an annual turnover of over INR 40,00,000 (Indian Rupees forty lakh) or an annual export turnover of more than INR 5,00,000 (Indian Rupees five lakh); and

   b) the third party is the actual 'payee that interfaces with the payer for the underlying transaction'.

2. **What has changed**: The New PA Directions mark a significant shift in RBI's position in the Draft PA Amendments on third-party payouts, allowing them under specific, qualified conditions. The Draft PA Amendments had expressly banned third-party payouts. In response to specific stakeholder feedback, RBI has decided to allow third-party payouts subject to certain restrictions.

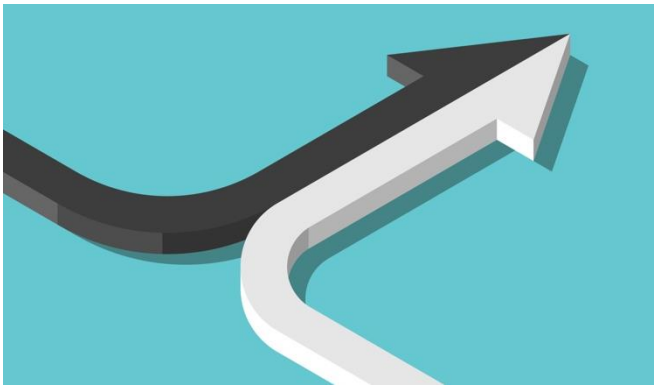
3. **Practical implications**: This provision appears to permit specific use in cases where a merchant directs a PA to settle funds directly to a third party. The phrase "*interfaces with the payer*" is crucial, defining the scope of these settlements. This new rule seems to allow for settlements to entities that directly interact with the customer (the payer) for the delivery of goods or services. A classic example is a marketplace or travel aggregator model.

    a) Scenario: A customer pays an e-commerce platform (the merchant) for a product sold by a third-party seller. The PA, which has a contract with the e-commerce platform, can now settle the funds directly into the seller's bank account.

    b) Key distinction: Previously, PAs could settle to any third party based on the merchant's instructions. However, the New PA Directions impose a critical condition, wherein the third party must be the one who "*interfaces with the payer*". This narrows the scope of permitted debits. Additionally, the instructing merchant must meet the specific annual turnover requirement.

Importantly, other broader use cases, such as a merchant using a PA to pay its vendors or employees, are not permitted under New PA Directions. The phrase 'interfaces with the payer' seems to explicitly exclude these scenarios.

Notably, Chapter IV, Paragraph 13(g) of the New PA Directions states that funds due to a merchant should be credited only to the merchant's own bank account. This appears to be a drafting oversight that directly contradicts the explicit permission for third-party payouts found under 'permitted debits' in Chapter V, Paragraph 16a of the New PA Directions. This contradiction could create confusion regarding the correct application of the rules.



PA partnering with another PA

The New PA Directions clarifies the regulatory position on PAs partnering with one another, a crucial development that validates and formalises certain industry practices.

1. **New provision**: The New PA Directions explicitly permit a PA to partner with another PA for specific functions, such as merchant due diligence and settlement. This provision introduces a clear framework for a PA contracting with another PA, which supports the industry practice of PA-to-PA arrangements.

2. **What has changed**: In the Draft Amendments, RBI had stated that for a payment transaction facilitated by 2 (two) or more authorised PAs, all PAs in the transaction chain would be subject to RBI's instructions. This is diluted in the New PA Directions, which now clearly delegates the due diligence and KYC responsibility to the PA that directly onboards the merchant. The New PA Directions also explicitly list 'Payment to another PA or PA-CB' as a permitted debit from the escrow account, formal recognition of inter-PA fund flows.

3. **Practical implications**:

    a) KYC and due diligence: The New PA Directions clarify that the PA directly onboarding a merchant is solely responsible for its due diligence and KYC, even if the primary PA is the one managing the payment flow. This aligns with existing market practice where a primary PA receives the KYC records from a sub-aggregator.

    b) Formalised fund flow: The explicit inclusion of inter-PA payments as a permitted debit from the escrow account provides a formal regulatory basis for such arrangements. This addresses the practical need for fund flow between aggregators in complex transactions, such as when a domestic PA uses a cross-border PA to facilitate an international payment.

    c) No dual KYC: As a result of this clarification, both PAs in a partnership do not need to perform due diligence and KYC on the same merchant, which reduces operational redundancy and cost. However, other compliances still apply to both PAs.

PA merchant agreement

1. **New provision**: The New PA Directions state that the agreement between a PA and its merchants must be 'fair and equitable' and transparently mention the settlement timelines.
2. **What has changed**: Earlier, settlement timelines were prescribed by RBI. Now, while RBI has specified a high-level framework, the exact timelines are to be determined and agreed upon in the merchant agreement itself.
3. **Practical implications**: This gives merchants a stronger position to negotiate better terms and settlement schedules with PAs, as the agreement is now legally required to be fair and equitable. This provides greater flexibility and control to the merchant over their cash flow.

Merchant due diligence and KYC

1. **New provision**: The New PA Directions mark a significant shift in merchant due diligence and KYC for PAs. It is more uniform and robust, ending previous exemptions and introducing a mandatory, tiered approach that balances strict compliance with the needs of small businesses. A 2 (two) step approach to merchant verification is introduced:
   a) Mandatory CKYCR integration: PAs are now required to retrieve merchant KYC records from the CKYCR. It appears that this step aims to streamline verification and ensure a centralised, consistent approach to identity management.
   b) Alternative verification: If a merchant's records are not available in the CKYCR, PAs can conduct due diligence through alternative mechanisms outlined in the KYC MD 2016. This includes using e-KYC with Aadhaar, offline Aadhaar verification, or verifying OVDs such as e-Permanent Account Number ("**PAN**") or documents from DigiLocker.

   For smaller merchants, the New PA Directions provide a simplified KYC process, though its specific application is not entirely clear. A simplified CDD process can be adopted for merchants with an annual turnover of up to INR 40,00,000 (Indian Rupees forty lakh) (or export turnover not exceeding INR 5,00,000 (Indian Rupees five lakh).
2. **What has changed**: Previously, PAs were exempt from performing mandatory CDD on merchants. This was due to the 2020 PA Directions, and the subsequent clarifications issued thereunder, which did not consider a PA-merchant relationship to be an 'account-based' relationship - one that would necessitate full CDD. The New PA Directions remove this exception and make CDD mandatory for all merchants, which in turn mandates PA's integration with CKYCR. PAs must now conduct a CDD on their merchants in accordance with the KYC MD 2016.

   For smaller merchants, while the Draft PA Amendments had different simplified KYC standards for 'small' (i.e. turnover of less than INR 5,00,000 (Indian Rupees five lakh) and 'medium' (i.e. turnover of less than INR 40,00,000 (Indian Rupees forty lakh) merchants, the New PA Directions appear to consolidate and toughen these requirements. Now, for all merchants under the INR 40,00,000 (Indian Rupees forty lakh) turnover threshold, the simplified KYC requires:
   a) contact point verification;
   b) verification of an OVD; and
   c) PAN verification.
3. **Practical implication:** While the New PA Directions provide welcome thresholds for simplified KYC, they do not clarify the method of verification for a merchant's turnover. The obvious question is whether PAs are expected to independently verify the turnover or if a declaration from the merchant would suffice. Furthermore, the New PA Directions do not address the scenario where a merchant's turnover increases mid-way through the relationship, crossing the INR 40,00,000 (Indian Rupees forty lakh) or INR 5,00,000 (Indian Rupees five lakh) threshold. These ambiguities could impact a PA's ability to manage its KYC compliance program effectively and may also have a direct bearing on the third-party payout rule for these merchants, which is also tied to turnover thresholds.

Oversight on merchant-displayed information

1. **New provision**: The New PA Directions state that a PA must ensure that any charges, other than the price of goods, services, or investment amount, charged by a merchant are distinctly displayed to the payer prior to the transaction.
2. **Practical implication**: This raises a crucial question as to the extent of a PA's oversight. While this obligation can be factored into a merchant agreement, a PA's control and visibility typically begin at the checkout page, after the merchant has already displayed the final price and any additional charges. This creates an operational challenge, as a PA cannot feasibly monitor every aspect of a merchant's website or physical point of sale to ensure compliance with this provision. Without real-time pre-checkout monitoring capabilities, a PA's ability to enforce this rule is limited.

PA-CB specific provisions

1. **New provision**: The New PA Directions consolidate previous circular on cross-border payments into a single document. They explicitly state that PA-CB funds for inward and outward transactions must be kept separate, with no co-mingling or netting off permitted. The maximum value per transaction for a PA-CB has been changed from 'per unit of goods or services' to a single limit of INR 25,00,000 (Indian Rupees twenty-five lakh) per transaction, which can be onerous for cross-border PAs.
2. **What has changed**: The explicit prohibition of co-mingling of funds and netting off for inward and outward transactions is a new provision that formalises a practice already understood and followed by the industry. The change in the transaction value limit from 'per unit' to 'per transaction' appears to be a significant change that could impact merchants selling multiple high-value items in a single transaction.
3. **Practical implications**: The New PA Directions further state that a "*payment transaction shall be identified as a cross-border transaction*". This seems to suggest that the entire payment ecosystem, including the PA-CB, its acquiring bank, and the payment service providers, must be able to recognise and flag these transactions to ensure proper handling and reporting. While this is already an existing practice for Export Data Processing and Monitoring System/Import Data Processing and Monitoring System reporting, the provision's inclusion in the New PA Directions makes it a formal regulatory requirement.

Conclusion

The New PA Directions is a significant step towards consolidating and standardising regulations for the growing payments industry. It addresses many of the ambiguities from the Draft PA Amendments, particularly regarding third-party payouts, capital requirements, and due diligence for smaller merchants. While it provides welcome clarity and formalises existing market practices, certain areas, such as the classification of hybrid physical/online transactions and the wording around simplified KYC, still have elements of ambiguity that may require further clarification from RBI or a test of time through industry practice.

RBI issues directions on authentication mechanisms for digital payment transactions

RBI, on September 25, 2025, issued the RBI (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, mandating 2 (two)-factor authentication ("**2FA**") across all digital payment modes. The norms follow a draft circular released in February 2024 and require the use of secure, dynamic authentication factors, moving beyond reliance on SMS-based OTPs.

Under the revised framework, all digital payments, including UPI, cards, wallets, net banking, NEFT, IMPS, and account transfers, must undergo 2FA, except for

card-present transactions. At least 1 (one) authentication factor must be dynamically generated or proven to be unique to each transaction. While SMS-based OTPs may still be used, RBI encourages the adoption of advanced methods such as biometrics, app-based tokens, and device-native authentication.

Certain categories remain exempt from mandatory 2FA, including small-value contactless payments, recurring e-mandate transactions (post-registration), specified PPI transactions, PPI gift cards, National Electronic Toll Collection (NETC) toll payments, and travel bookings via International Air Transport Association (IATA)-approved global distribution systems. The norms do not apply to cross-border digital payments; however, card issuers must now validate non-recurring cross-border card-not-present transactions, register their bank identification numbers with card networks, and implement risk-based controls for such transactions.

RBI issues Master Directions on Digital Banking Channels Authorisation

On November 28, 2025, RBI issued the RBI (Digital Banking Channels Authorisation) Directions, 2025 ("**Digital Banking Directions**"), establishing a consolidated regulatory framework for digital banking services offered by commercial banks, effective January 1, 2026.

The Digital Banking Directions distinguish between 'view-only' and 'transactional' facilities. While eligible banks can launch view-only services by notifying RBI via the PRAVAAH portal within 30 (thirty) days along with a certified Gap Assessment and Internal Controls Adequacy ("**GAICA**") report, transactional services require prior RBI approval. Banks seeking transactional authorisation must demonstrate higher financial stability, specifically adhering to capital adequacy ("**CRAR**") norms and net-worth requirements, in addition to the baseline Core Banking Solution ("**CBS**") and IPv6 readiness prerequisites. Operationally, the Digital Banking Directions emphasise consumer protection by mandating explicit customer consent for registration and strictly prohibiting the mandatory bundling of digital banking services with other products, such as debit cards. It also incorporates the Ministry of Finance's 'Accessibility Standards in the Banking Sector' and requires terms and conditions to be provided in English, Hindi, and local languages. Notably, RBI has introduced a significant compliance relief; banks with an existing authorised digital channel do not require fresh approval to launch additional channels, provided they continue to comply with the master directions on information technology governance, outsourcing, and fraud risk management.

RBI issues Consolidated Master Directions, 2025

In a landmark regulatory overhaul, on November 28, 2025, RBI streamlined the regulatory architecture by consolidating over 9,000 (nine thousand) existing circulars and guidelines into 244 (two hundred and forty-four) function-wise master directions. The exercise, aimed at enhancing the ease of doing business and reducing compliance burdens, involves the repeal of 5,673 (five thousand six hundred and seventy-three) obsolete circulars and the incorporation of 3,809 (three thousand eight hundred and nine) circulars into the new master directions. These consolidated directions are categorised by RE type (e.g., commercial banks, non-banking financial companies, payment banks) and function, serving as the single authoritative source for regulatory instructions. While the consolidation largely retains the 'as-is' regulatory position to ensure continuity, it eliminates ambiguities arising from overlapping circulars and introduces a uniform structure for future amendments.

National Payments Corporation of India

Introduction of additional requirements for UPI Circle Full Delegation Framework

The National Payments Corporation of India ("**NPCI**") issued an addendum on July 8, 2025, to its earlier circular on UPI Circle – Delegated Payments. The

addendum introduces enhanced requirements under the 'Full Delegation Framework', building upon the circular dated August 13, 2024. It focuses on improving identification, verification, and consent processes when primary users authorise secondary users to make transactions within defined spend limits.

The updated framework now requires primary users to restrict delegation to specific segments such as family members or domestic/small business employees. PSPs are also required to share additional documentation details, including document type and ID number, with the secondary payer PSP and the issuer bank. Issuer banks are required to verify secondary users using name, mobile number, and identification number from an OVD under the KYC MD 2016.

Further, secondary payer PSPs are required to obtain explicit consent from secondary users for the collection of such additional details before processing delegation requests. NPCI directed all UPI member banks, PSPs, and third-party app providers to update their systems and implement these changes by August 31, 2025.

Ministry of Electronics and Information Technology

Digital Personal Data Protection Rules, 2025: Operationalising consent, security, and governance obligations

The Government of India has officially notified the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") on November 13, 2025, published in the official gazette on November 14, 2025. The DPDP Rules enable the operationalisation of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**").

The DPDP Act is India's first comprehensive, principles-based statute governing the processing of digital personal data. It applies to processing within India and extraterritorially to entities offering goods or services to individuals in India. The DPDP Act operates primarily on a foundation of explicit consent.

The DPDP Rules *inter alia* include key operational rules for Data Fiduciaries[1] ("**Data Fiduciary**") and addresses mechanisms created to protect the rights of Data Principals[2] ("**Data Principal**").

Phased commencement of key provisions

The DPDP Rules implement a staggered approach to commencement, a critical factor for global compliance planning:

Timeline	Commencement date	Implication
Immediate	November 13, 2025	Establishment of the Data Protection Board of India ("**Board**") and its operational procedures.
12 months	November 13, 2026	The framework for the registration and detailed obligations of Consent Managers ("**Consent Managers**"), the term used for a person registered with the Board, to act as a point of contact to enable a Data Principal to give, manage, review and withdraw consent, comes into force.
18 months	May 13, 2027	Core compliance duties apply, including notice, security safeguards, breach intimation, Significant Data Fiduciary ("**SDF**") obligations, and Data Principal rights.

[1] Data Fiduciaries is the term used for entities that determine the purpose and means of processing (analogous to 'data controllers' in other regimes).

[2] Data Principals is the term used for individuals to whom the personal data relates (analogous to 'data subjects' in other regimes).

Critical compliance obligations for Data Fiduciaries

The DPDP Rules set out the operational requirements that Data Fiduciaries must follow to implement the core obligations under the DPDP Act.

Notice and consent

The formal notice provided by a Data Fiduciary to a Data Principal must be clear, independent, and contain a 'fair account' of the processing activities. The overall framework is grounded in a notice-and-consent model, requiring Data Fiduciaries to disclose key processing details upfront and obtain valid consent before processing begins. The notice requires, at minimum:

1. an itemised description of the personal data to be processed;
2. the specified purpose of processing, including a specified description of the goods, services, or uses enabled; and
3. a specific communication link for Data Principals to withdraw consent, exercise other rights or make a complaint to the Board, ensuring the ease of withdrawal is comparable to the ease with which consent was given.

Business impact

Organisations will need to redesign consent flows and user interfaces to ensure consent is purpose-specific, informed with clear withdrawal pathways, or at the very least update their privacy policies to include the foregoing.

Security safeguards and breach intimation

The DPDP Rules mandate enhanced security and stringent breach reporting protocols:

1. **Mandatory security measures**: Data Fiduciaries must implement minimum safeguards, including encryption, obfuscation, masking, or the use of virtual tokens. This applies to all personal data held or controlled, including personal data processed by a Data Processor (entity processing personal data on behalf of the Data Fiduciary) ("**Data Processor**").
2. **Contractual mandate**: Contracts with Data Processors must contain appropriate provisions for implementing these reasonable security safeguards.
3. **Time-bound breach reporting**: Upon becoming aware of a personal data breach, a Data Fiduciary must:
   a) intimate and provide the Board a description of the personal data breach without delay, followed by a detailed report within 72 (seventy-two) hours; and
   b) intimate each affected Data Principal without delay, providing a description of the breach, its consequences, and mitigation measures.

Business impact

Companies will need to implement appropriate data security safeguards across all systems handling Indian personal data. Coupled with steep penalties of up to INR 200,00,00,000 (Indian Rupees two hundred crore) (~ USD 22,200,000 (US Dollars twenty-two million two hundred thousand) for reporting failures and the stringent 'without delay' notification requirement, organisations will likely need to operationalise a round-the-clock, India-aligned incident response function and incorporate strong, protective indemnity clauses in their Data Processor contracts to mitigate liability exposure.

Data retention and erasure

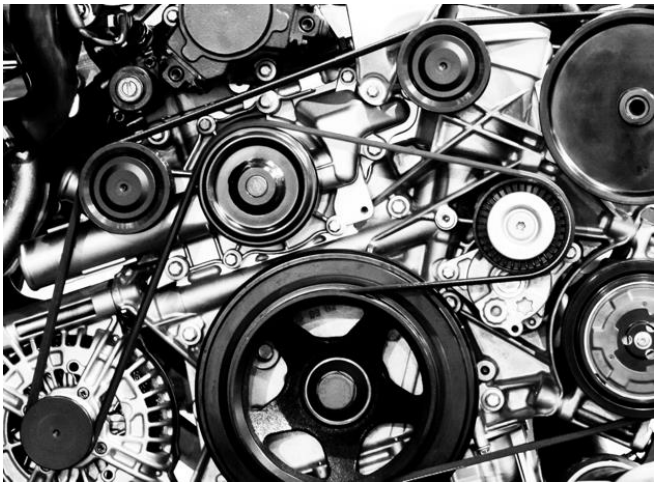
The purpose of limitation principle, that personal data should only be kept as long as necessary for the specified purpose, is made quantifiable for certain large-scale Data Fiduciaries:

1. **Retention period for large fiduciaries**: E-commerce entities (with a minimum of 20,000,000 (twenty million) users), online gaming intermediaries (with a minimum of 5,000,000 (five million) users), and social media intermediaries (with a minimum of 20,000,000 (twenty million users) must erase personal data (with exceptions for user account access and virtual tokens) within 3 (three) years of the date, the Data Principal last approached the Data Fiduciary for the specified purpose, unless retention is mandated by law.

2. **Mandatory log retention**: Data Fiduciaries must retain associated traffic data and other processing logs for a minimum period of 1 (one) year for forensic and investigative purposes, after which they must be erased.
3. **Erasure notice**: Data Fiduciaries must notify Data Principals at least 48 (forty-eight) hours prior to the completion of the time period for erasure, allowing the Data Principal a chance to engage with the Data Fiduciary to preserve the personal data.

Business impact

The DPDP Rules adopt a highly prescriptive approach to data retention, introducing a defined 3 (three) year deletion timeline for certain large digital platforms. This could require significant operational adjustments. Large e-commerce, gaming, and social media intermediaries will need to re-engineer data lifecycle practices, implement automated and auditable deletion workflows, and build mechanisms to track a Data Principal's 'last approach' date with precision.



Key new regulatory mechanisms

Consent Manager framework

The Consent Manager framework is operationalised as a key intermediary to empower Data Principals:

1. **Registration criteria**: The stringent conditions ensure only trustworthy entities qualify. Requirements include: incorporation in India; minimum net worth of INR 2,00,00,000 (Indian Rupees two crore) (~ USD 200,000 (US Dollars two hundred thousand); demonstration of sufficient technical, operational, and financial capacity; and certification that its platform is interoperable and adheres to data protection standards.
2. **Fiduciary capacity**: A Consent Manager must act in a fiduciary capacity toward the Data Principal.
3. **Obligations**: Consent Managers are prohibited from sub-contracting their obligations, must avoid conflicts of interest with Data Fiduciaries. Consent Managers must retain a record of consents, notices, and data sharing activities for at least 7 (seven) years. Critically, the Consent Manager cannot read the contents of the personal data being shared.

Business impact

The Consent Manager construct, unique to the DPDP Act regime, creates a new consent orchestration layer. This introduces both compliance and architectural implications. Organisations may opt to build technical integrations with registered Consent Managers, redesign data-sharing workflows to route consent tokens through the Consent Manager ecosystem and accommodate 7 (seven) year retention requirements for consent records. Data Fiduciaries will need to establish robust governance and verification processes before relying on any Consent Manager. This necessity arises from the constraints on Consent Managers, which include inability to sub-contract, fiduciary duties towards Data Principals, and the imperative to remain conflict-free. Overall, the framework adds a significant new dependency for lawful, consent-driven processing and may materially influence product design, user experience, and backend data management practices.

SDF additional obligations

The Central Government may notify Data Fiduciaries as SDFs based on criteria like the volume and sensitivity of personal data processed. Once notified, these entities face enhanced scrutiny:

1. **Mandatory annual assessment**: SDFs must conduct a Data Protection Impact Assessment ("**DPIA**") and an audit once every 12 (twelve) months.
2. **Algorithmic due diligence**: SDFs must exercise due diligence to verify that technical measures, including algorithmic software used for processing, do not pose a risk to Data Principals' rights.

3. **Data localisation restriction**: SDFs must undertake measures to ensure that certain personal data, when specified by the Central Government, is not transferred outside the territory of India. This potential restriction is based on the recommendation of a government-constituted committee.

Business impact

While the DPIA concept mirrors elements of the General Data Protection Regulation ("**GDPR**") under European laws, the SDF designation introduces a far more intensive, India-specific compliance burden. Once classified as an SDF, an organisation needs to operationalise annual DPIAs and audits, implement ongoing algorithmic risk assessments, and prepare for the possibility of strict data-localisation obligations for categories of personal data that may be notified by the Government. At the moment, there is no clarity on what additional localisation obligations will be imposed. Notably, sectoral localisation obligations, such as payments data localisation, continue to apply

International transfers and vulnerable data

Cross-border data transfer

The DPDP Rules affirm the liberalised approach to personal data transfer. Accordingly:

1. personal data processed under the DPDP Act may be transferred outside the territory of India; and
2. permission is subject to any restrictions that the Central Government may specify by general or special order concerning making personal data available to any foreign State or entity under its control. This maintains the 'blacklist' approach, providing operational ease until any prohibitive list is notified.

Business impact

India's continued use of a 'blacklist' model, where cross-border transfers are permitted unless a country or entity is specifically restricted, offers far greater operational flexibility than the GDPR's adequacy and standard contractual clauses-based framework. For businesses, this could mean faster and lower-cost international data flows, with fewer contractual and assessment burdens, except in situations where additional localisation obligations are applicable to the data or entity in consideration.

Processing of child data and PwD data

1. **Verifiable consent**: Processing the personal data of a child (an individual under 18 (eighteen) years of age) or a PwD requires verifiable consent from the parent or lawful guardian.
2. **Verification**: Data Fiduciaries must adopt appropriate technical and organisational measures to verify that the individual claiming to be the parent is an identifiable adult. This verification is often by reference to reliable identity and age details or a virtual token issued by an authorised entity.
3. **Exemptions**: Limited exemptions from the parental consent and protective duties are provided to certain classes of Data Fiduciaries (e.g., clinical establishments, educational institutions) for purposes such as providing health services or ensuring child safety and protection.

Business impact

The DPDP Rules require platforms, handling child or disability-related personal data to implement reliable parental consent verification systems, adding technical and operational overhead. Product flows, especially for gaming, ed-tech, and social platforms, will need stronger age-gating, guardian consent paths, and restricted processing by default. Even with limited exemptions, most businesses must introduce special handling and governance controls for such personal data to remain compliant.

Conclusion

The DPDP Rules operationalise India's new data protection regime by introducing detailed, prescriptive requirements that will require significant operational, technical, and governance adjustments for organisations processing personal data in India.

While the staggered timelines offer some room for transition, businesses, especially large digital platforms and entities likely to be designated as SDFs, will need to begin alignment efforts well in advance of the 2027 compliance date. The DPDP Rules also create new ecosystem dependencies, such as the Consent Manager framework, and introduce India-specific obligations around breach reporting, retention, and algorithmic due diligence. Overall, the DPDP framework represents a material shift toward structured and enforceable data governance, demanding early planning, cross-functional coordination, and sustained compliance readiness.

Quick Snapshots

1. **Registered intermediaries now permitted to use the 'e-KYC Setu System' of NPCI**: Registered intermediaries currently use Unique Identification Authority of India ("**UIDAI**") e-KYC services in the securities market. Digital KYC verification has been undertaken using the KYC User Agency mechanism, and/or Digilocker. SEBI, *vide* press release dated June 30, 2025, announced that registered intermediaries can now use the 'e-KYC Setu System' developed by the UIDAI along with NPCI to perform digital KYC verification and ease the process of customer onboarding digitally. This facility acts as an alternate mechanism to undertake Aadhaar-based e-KYC of their clients.

2. **RBI guidelines for due diligence and monitoring of Aadhaar Enabled Payment System ("AePS") operators**: In a move to strengthen security and compliance in AePS transactions, RBI, on August 14, 2025, issued detailed guidelines for the due diligence of AePS Touchpoint Operators ("**ATOs**"). Under the new directives, acquiring banks must conduct a thorough KYC verification of ATOs before onboarding. It must conduct periodic updates and re-verification if ATOs remain inactive for over 3 (three) months. Banks are also required to continuously monitor ATO activities using transaction monitoring systems. It must impose risk-based operational limits and regularly review these parameters in line with emerging fraud trends. Further, strict system-level controls must be in place to ensure that technological tools such as Application Programming Interfaces ("**APIs**") are used exclusively for AePS operations.

3. **Success story from the fifth cohort of RBI regulatory sandbox**: In the fifth cohort of RBI regulatory sandbox, 5 (five) entities were selected to test their products. Out of the products that completed the test phase, the blockchain based deep-tier financing solution proposed by Indian Banks' Digital Infrastructure Company Private Limited ("**IDBIC**") was found viable. The product enables micro, small, and medium enterprises within a creditworthy anchor's supply chain to access affordable finance. The platform functions by tokenising the Tier-1 supplier invoice upon its acceptance by the anchor, against which lenders can digitally provide funds.

4. **RBI establishes Regulatory Review Cell ("RRC") to streamline regulatory reforms**: RBI has set up a RRC within its Department of Regulation to streamline regulatory changes and expedite the review process. As part of this initiative, RBI has also constituted an independent 'Advisory Group on Regulation', chaired by Mr. Rana Ashutosh Kumar Singh, Managing Director, State Bank of India, along with 5 (five) other financial sector executives, to channel industry feedback on regulations to the RRC. The RRC will ensure that RBI regulations are reviewed every 5 (five) to 7 (seven) years, thereby enabling a more systematic and comprehensive approach to regulatory

updates, which were earlier effected primarily through circulars.

5. **Ministry of Communications launches UPI - Universal Postal Union ("UPU") integration project to enhance cross-border remittances**: The Ministry of Communications unveiled the UPI-UPU integration project, an initiative aimed at transforming cross-border remittances for millions worldwide. Developed jointly by the Department of Posts, NPCI International Payments Limited, and the UPU, the project integrates India's UPI with the UPU interconnection platform, combining the extensive reach of the postal network with the speed and affordability of UPI.

6. **The International Financial Services Centres Authority ("IFSCA") signs Memorandum of Understanding ("MoU") with Australian Securities and Investments Commission ("ASIC") to enhance regulatory cooperation**: IFSCA and ASIC have entered into an MoU to strengthen inter-regulatory cooperation and promote a robust and effective financial services ecosystem in both jurisdictions. The MoU aims to facilitate mutual assistance and information sharing between the regulators on trends and best practices relating to financial market regulation, the use of technology, and other areas of mutual interest. It will also enable the timely exchange of information on key developments concerning financial services, regulatory compliance, supervision, and enforcement of market participants.

7. **RBI grants Paytm payments services authorisation to operate as a PA-O**: RBI authorised Paytm Payments Services to operate as a PA-O. This authorisation removes the earlier restrictions on onboarding merchants.

8. **NPCI introduces 'RDS' sub-product for Retail Direct Scheme**: NPCI introduced a new ACH Debit sub-product titled 'RDS' on November 6, 2025. This initiative is designed to support the processing of transactions under RBI's Retail Direct Scheme, enabling individual investors to directly invest in government securities with greater ease by standardising the mandate registration process.

9. **Central Registry of Securitisation Asset Reconstruction and Security Interest ("CERSAI") authorised for voluntary Aadhaar authentication**: The Department of Financial Services, *vide* notification dated November 6, 2025, authorised the CERSAI to conduct voluntary Aadhaar-based authentication. This allows CERSAI, as the CKYCR, to verify demographic details for entities regulated by RBI, SEBI, and the Insurance Regulatory Development Authority of India, provided an explicit consent is obtained from the customer, thereby reducing the friction in retrieving KYC records.

10. **SEBI issues caution on 'Digital Gold' products**: SEBI, in a press release dated November 8, 2025, cautioned investors against online platforms offering 'Digital Gold' or 'E-Gold' products. SEBI clarified that these products are neither recognised as securities nor regulated as commodity derivatives and thus do not carry the investor protection safeguards available in regulated markets, advising investors to exercise due diligence.

11. **MeitY releases 'India AI Governance Guidelines'**: On November 5, 2025, MeitY released the 'India AI Governance Guidelines' under the India AI Mission. The guidelines outline 7 (seven) ethical principles and 6 (six) governance pillars to ensure the responsible development and deployment of AI technologies in India, emphasising the need for transparency in algorithmic decision-making and non-discriminatory outcome testing.

12. **NPCI introduces AI-powered 'UPI HELP Assistant'**: NPCI has launched the 'UPI HELP Assistant', a pilot program utilising a proprietary financial domain-specific AI model to provide intelligent conversational support to users. This assistant enables users to resolve digital payment queries, track transaction status, log complaints, and manage mandates through simple keywords and deep links to UPI apps. Banks and PSPs are required to prominently display links to the assistant on their official channels and ensure the timely resolution of complaints received through this mechanism.

13. **NPCI extends UPI Circle framework to Internet of Things ("IoT") devices**: NPCI has issued an addendum extending the UPI Circle - Delegated Payments facility to IoT devices and software profiles under the Full Delegation Framework. This allows primary users to authorise up to 5 (five) secondary IoT devices or software profiles for domestic Person-to-Merchant transactions, subject to a monthly limit of INR 15,000 (Indian Rupees fifteen thousand) and a per-transaction limit of INR 5,000 (Indian Rupees five thousand). The framework mandates close proximity during linking, introduces a 24 (twenty-four) hour cooling period with restricted limits, and assigns a specific purpose code 'BH' for settlement and reconciliation.

FinTech Practice

JSA is one of India's pioneering law firms in the FinTech space. JSA's FinTech group brings together an integrated multi-practice team to support clients with transactions, disputes and regulatory matters at the intersection of financial services and technology. Our practice leverages the experience and in-depth technology expertise of attorneys across practice areas and allows us to offer clients access to time-tested strategies and holistic advice. Our experienced attorneys are well positioned to assist clients navigate through the complex legal, regulatory and compliance landscape within which these businesses and their technologies operate. Our strong relationships with regulators, banks, insurers, funds, large technology companies and infrastructure and service providers mean that we understand the issues that affect every area of the financial technology ecosystem. This enables us to deliver incisive, informed and innovative advice across the FinTech spectrum. We work with financial institutions, as they adapt and transform, FinTech start-ups, from inception through to all rounds of funding, to IPO and beyond, large technology companies diversifying into FinTech and Investors and strategic acquirers as they identify and secure strategic opportunities in the FinTech space.

Our areas of expertise inter alia include: (a) Prepaid payment instruments and variations thereof, (b) Remittance (person-to-person and person-to-merchant) models and services, (c) Central treasury arrangements and collection agency models, (d) Artificial Intelligence (AI) and Machine Learning (ML) enabled payment systems, (e) Alternative lending and payment platforms, (f) blockchain enabled service offerings, including smart contracts, (g) crowdfunding and crowdsourced investments, (h) Cryptocurrencies, including initial coin offerings, (i) InsurTech products and business models, (j) investments, including PE/VC financing into fintech and financial services companies, (k) Invoice trading and receivable discounting platforms, (l) Payment services and solutions (both cross-border and domestic).

The authors of this Compendium are:

Probir Roy Chowdhury
Partner

Sajai Singh
Partner

Yajas Setlur
Partner

19 Practices and
40 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

15 Practices and
20 Ranked Lawyers

13 Practices and
49 Ranked Lawyers

20 Practices and
24 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Regional Legal Expertise Awards (APAC) of the Year
Energy Firm Competition/
Antitrust Firm

Among Best Overall
Law Firms in India and
14 Ranked Practices
---
9 winning Deals in
IBLJ Deals of the Year
---
15 A List Lawyers in
IBLJ A-List – 2026

Recognised in World's 100 best
competition practices of 2026

Ranked Among Top 5 Law Firms in
India for ESG Practice

Asia M&A Ranking
2025 – Tier 1

For more details, please contact km@jsalaw.com

www.jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi