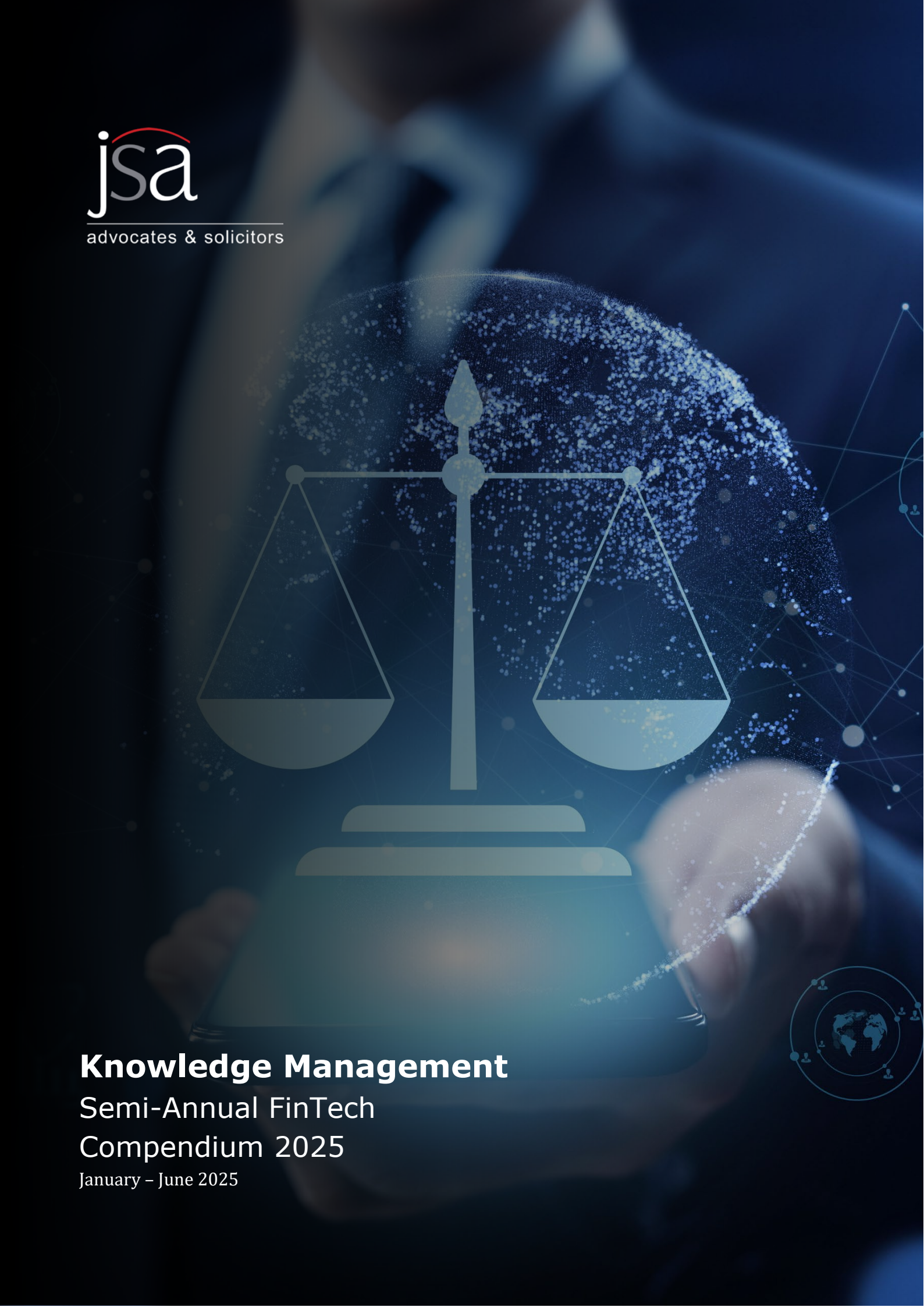
jsa
advocates & solicitors



Knowledge Management

Semi-Annual FinTech Compendium 2025

January – June 2025

Semi-Annual FinTech Compendium 2025

Introduction

This Compendium consolidates all the key developments pertaining to FinTech sector in India which were circulated as a part of the JSA Prisms and Newsletters during the calendar period from January 2025 till June 2025.

Reserve Bank of India

Reserve Bank of India introduces draft circular on Additional Factor of Authorisation for cross-border Card Not Present transactions

Following the Reserve Bank of India's ("**RBI**") February Statement on Developmental and Regulatory Policies, it has introduced a draft circular on Additional Factor of Authorisation ("**AFA**") for international Card Not Present ("**CNP**") transactions.

Since 2009, RBI has required AFA for domestic CNP transactions, while exempting international transactions from this requirement. Many merchants utilised the AFA exemption for international CNP transactions by using foreign acquirers to facilitate payments for domestic transactions – in light of which, RBI issued a circular in 2014 stating:

"[W]*here cards issued by banks in India are used for making card not present payments towards purchase of goods and services provided within the country, the acquisition of such transactions has to be through a bank in India and the transaction should necessarily settle only in Indian currency, in adherence to extant instructions on security of card payments.*"

Now, RBI intends to align the framework for authenticating international CNP transactions (i.e., for purchase of goods and services provided from outside India using a card issued by an Indian issuer) with the domestic framework, requiring AFA for such transactions as well. This framework will require card issuers to register their bank identification numbers with card networks for AFA validation.

RBI releases the framework for imposition of penalties and compounding under the Payment and Settlement Systems Act, 2007

RBI has released the Framework for imposing monetary penalty and compounding of offences under the Payment and Settlement Systems Act, 2007 ("**PSS Act**"), superseding its earlier circular dated January 10, 2020. This updated framework, effective immediately, reflects amendments to the PSS Act. This development provides greater clarity and formalises RBI's approach to enforcing compliance within the payment ecosystem. It details the process for compounding certain offences under the PSS Act, offering a mechanism for resolution prior to or during formal proceedings. Eligible contraventions (excluding those punishable solely by imprisonment), may be subject to compounding upon application to RBI. The determination of the compounding amount will be based on principles similar to those governing penalties, with a potential reduction of 25%. However, repeated contraventions will attract higher compounding fees. The framework emphasises that the submission of a compounding application does not guarantee its acceptance. Entities subject to monetary penalties or compounding actions will be required to disclose these details in their annual financial statements, and RBI will also issue public disclosures. It underscores RBI's commitment to ensuring robust compliance within the payment and settlement systems, providing regulated entities with a clearer understanding of the enforcement landscape and the available mechanisms for addressing non-compliance.

RBI invites applications for recognition of Self-Regulatory Organisation(s) for the Account Aggregator ecosystem

With an aim to have a dedicated Self-Regulatory Organisation(s) ("**SRO**") for the Account Aggregator ("**AA**") ecosystem, RBI, on March 12, 2025 released a Framework for Recognising Self-Regulatory Organisation(s) for the Account Aggregator Ecosystem (SRO-AA) ("**SRO-AA Framework**"),

Recognising the complexity of and increasing transactions within the AA ecosystem, RBI aims to foster a market-driven mechanism to address operational issues and promote sustainable development. RBI envisions SRO-AAs to be credible and independent bodies with the following key characteristics/responsibilities true representation of the ecosystem; establishment of codes of conduct and oversight mechanisms; development-oriented approach; independence from undue influence; and provision for grievance redressal and dispute resolution.

To be recognised, an SRO-AA must meet the specific eligibility criteria as mentioned below:

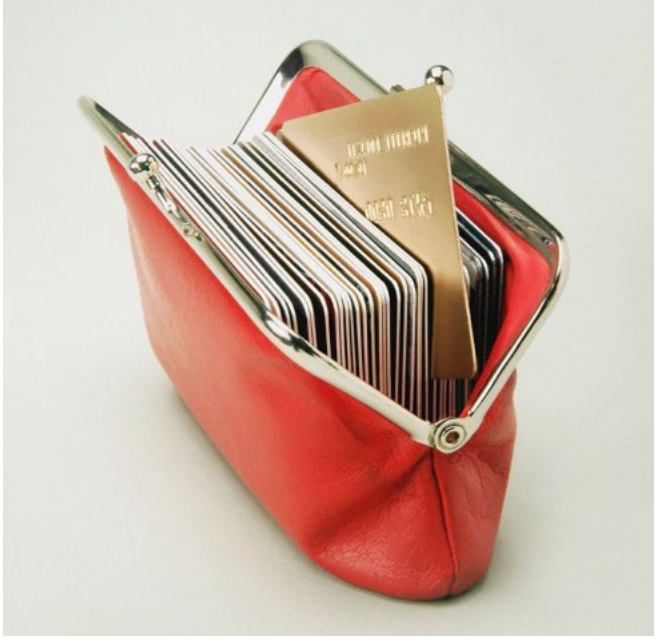
1. be a not-for-profit company under Section 8 of the Companies Act, 2013;
2. have, and thereafter, maintain a minimum net worth of INR 2,00,00,000 (Indian Rupees two crore) (approx. USD 231,000 (US Dollars two hundred and thirty-one thousand) within 1 (one) year after recognition as an SRO-AA or before commencement of operations as an SRO-AA, whichever is earlier;
3. have diversified shareholding with no single entity holding 10% or more;
4. possess the necessary infrastructure and IT capabilities to deploy technological solutions; and
5. applicant and its key executives should have professional competence and a clean reputation.

Membership in an SRO-AA will be voluntary but encouraged for all AAs. SRO-AAs will also be expected to have a balanced representation of financial information providers and financial information users, with at least 25 (twenty-five) unique entities from each group.

SRO-AAs will have several key functions, including setting codes of conduct and benchmarks, overseeing member activities, promoting knowledge sharing and public awareness, facilitating common services and establishing dispute resolution mechanisms. Crucially, it will also act as a bridge between its members and RBI and other financial regulators, keeping them informed, providing data and adhering to their guidelines. RBI will oversee the recognition process and has the authority to revoke recognition if the SRO-AA's

functioning is detrimental or not in line with its objectives.

In conclusion, this framework lays a robust foundation for a self-governed and responsible AA ecosystem under RBI's oversight. By establishing clear criteria for SRO-AAs and outlining their crucial functions in setting industry standards, ensuring compliance and facilitating dispute resolution, RBI aims to foster a mature and efficient data-sharing environment. This initiative is expected to promote the orderly growth and stability of the AA ecosystem, fostering a collaborative environment where innovation can flourish within a framework of self-regulation. This allows AAs to proactively shape industry best practices and demonstrate responsible data handling, ultimately building greater trust and facilitating wider adoption of AA services.



New digital lending directions issued by RBI: A comprehensive overhaul of compliance norms

On May 8, 2025, RBI released comprehensive directions on digital lending by Regulated Entities ("**REs**") in India, i.e. the RBI (Digital Lending) Directions, 2025 ("**Digital Lending Directions**"). The Digital Lending Directions are not a revamp of the existing regulations, but a consolidation of the various instructions issued by RBI over the last few years with some key additions. The Digital Lending Directions supersede and replace the existing Guidelines on Digital Lending dated September 2, 2022, and the Guidelines on Default Loss Guarantee ("**DLG**") in Digital Lending dated June 8, 2023.

RBI sought to introduce accountability and transparency to a fast-growing industry which had concerns regarding the methods used to deliver and service digital credit products. It realised these concerns would impact the confidence of borrowers in digital lending in India. Therefore, after reviewing the recommendations made by the RBI constituted '*Working Group on Digital Lending*', RBI has issued the Digital Lending Directions.

Key provisions

Some of the important aspects covered under the Digital Lending Directions are:

1. **Definitions**: The definition of 'Lending Service Provider'("**LSP**") is revised to clarify that even another RE can be appointed as an LSP by an RE.
2. **Documentation and compliance requirements for appointment of LSPs**: REs are now required to enter into contractual agreements with LSPs. REs are also required to conduct periodic review of the LSP *vis-à-vis* the terms of such contractual agreements and take steps for any deviations. REs are now required to lay down, as part of its policy, suitable monitoring mechanisms for the loan portfolios originated with the support of LSPs.

   The Digital Lending Directions clarify that any outsourcing agreement entered into by the RE with an LSP will in no manner dilute or absolve the RE of its obligations under any statutory or regulatory provision, and the RE will remain fully responsible and liable for all acts and omissions of the LSP.
3. **Arrangements involving multiple lenders**: Additional compliance requirements have been set out for REs for those instances where the RE-LSP arrangement involves multiple lenders. These compliances include providing a digital view of all loan offers matching the borrower's requests which meets the borrower's requirements; and ensuring that the content displayed by LSPs are unbiased, objective and not promote the products of a specific RE, including through dark or deceptive patterns.
4. **Recovery of loans**: In contrast to the previous digital lending guidelines, RBI has recognised recovery related challenges and has permitted REs to use physical recovery agents to recover loans from delinquent borrowers in cash, whenever

necessary. In case of a default situation, REs are now required to notify the borrower (through email/SMS) about the particulars of recovery agents authorised by them, prior to such recovery agent approaching the relevant borrower for recovery of any loan.

5. **DLG arrangements:** RE need to now ensure that LSPs publish the details of DLG arrangements on the website of the relevant LSP on a monthly basis, by the 7th day of the subsequent month.
6. **Cooling off period**: Previously, borrowers were allowed to exit a digital loan by paying of the principal and the annual percentage rate without any penalty during an initial cooling off period. Now, REs may retain a reasonable one-time processing fee if the borrower exits the loan during such cooling off period. Additionally, the REs have been given the flexibility to set up a cooling off period of a minimum period of 1 (one) day as compared to the earlier requirement of a minimum period of 3 (three) days for loans with tenor of 7 (seven) days or more.
7. **Storage of data**: The previous regulations required all data to be stored only on servers located within India. The Digital Lending Directions have clarified that where data is processed outside India, it will be deleted and brought back to India within 24 (twenty-four) hours of processing such data.
8. **Reporting of Digital Lending Apps/Platforms ("DLAs")**: REs will report on the Centralised Information Management System ("**CIMS**") portal of RBI, the details of all DLAs deployed/joined by them, whether their own or those of the LSPs, either exclusively or as a platform participant. REs will update the list on the CIMS portal as and when additional DLAs are engaged by them or if the engagement with the existing DLA ceases.

Key timelines and dates

The Digital Lending Directions are effective from the date of their publication (May 8, 2025) except for the following:

1. the compliance requirements for all RE-LSP arrangements involving multiple lenders will come into effect from November 1, 2025; and
2. the reporting of all DLAs on the CIMS portal will be completed by all REs by June 15, 2025.

Conclusion

The Digital Lending Directions have introduced 2 (two) key new initiatives (increased transparency in digital loan aggregation and a public depository of DLAs) which should guide the digital lending industry on the path for sustainable and effective growth. It further represents a comprehensive regulatory intervention to balance innovation with consumer protection and systemic stability as well as prioritises and strengthens borrower trust. The Digital Lending Directions also aim to mitigate systemic risks by further regulating the LSP and DLG arrangements, stringent due diligence requirements for LSPs and the explicit liability of REs for any acts and omissions of the LSPs.

RBI releases new Know Your Customer Frequently Asked Questions

RBI has released Frequently Asked Questions ("**FAQs**") on Know Your Customer ("**KYC**") requirements applicable to its REs. The FAQs bring much-needed clarity relating to REs' KYC obligations. The FAQs clarify that if an existing KYC compliant customer of an RE desires to open another account or avail any other product/service from the same RE, he/she is not required to submit any new KYC documents unless there is a change to existing KYC information. Further, the FAQs clarify that Aadhaar is not mandatory for purposes of KYC.

The FAQs also distinguish between face-to-face onboarding and non-face-to-face onboarding – specifically classifying video-based customer identification process as face-to-face onboarding.

RBI updates the KYC Directions

RBI has amended its RBI (KYC) Directions, 2016 to now enable REs to use Business Correspondents ("**BCs**") to collect KYC self-declarations from customers. Such self-declarations may be obtained by BCs electronically, but until such option is made available, the declaration may be submitted in physical form by customers. BCs must authenticate the self-declaration and supporting documents submitted by customers and promptly forward the same to the concerned bank branch. BCs must also provide customers with an acknowledgment of receipt of such declarations/submission of documents.

In addition to the above, the amendment requires REs to intimate their customers in advance to update their respective KYC information. Prior to the due date to update KYC, REs must give at least 3 (three) advance intimations, including at least 1 (one) intimation in writing, to their customers. Even after the due date, REs must give at least 3 (three) reminders, including at least 1 (one) reminder in writing, to such customers if they have still not complied. The letter of intimation/reminder may, *inter alia*, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/reminder must be duly recorded in the RE's system against each customer for audit trail. All REs must comply with this requirement by January 1, 2026.

Securities and Exchange Board of India

Mandated safeguards for investor payments *via* Unified Payment Interface

On June 11, 2025, the Securities and Exchange Board of India ("**SEBI**") issued a circular introducing a secured Unified Payment Interface ("**UPI**") mechanism, specifically for investor-facing intermediaries to receive/collect funds from their investors ("**SEBI Circular**"). The SEBI Circular seeks to create a more structured framework towards increasing investor confidence in such systems.

Brief background

UPI, as a mode of payment in the securities market was first introduced in 2019[1]. However, in the last few years, SEBI has observed a significant increase of unregistered entities impersonating legitimate market intermediaries and misleading investors into transferring funds to unauthorised accounts for personal gains.

To curb these incidents, SEBI, in consultation with the National Payment Corporation of India ("**NPCI**"), has introduced a reliable UPI option to an investor to transfer funds directly to the verified bank account of registered intermediaries, by way of the issuance of the SEBI Circular. This proactive initiative by SEBI would help investors identify, isolate and avoid transferring funds to unregistered entities that do not have the unique UPI handles. The standardised and unique UPI handles would be available as an option for investors with effect from October 1, 2025.

Key features

As a part of this framework, SEBI has imposed the following security mechanisms:

1. **Validated UPI handles**:
    a) The unique, alphanumeric UPI ID will begin with a username selected by the intermediary that is readable and relatable to the intermediary.

[1] SEBI Circular dated November 1, 2018

b) The username will be followed by an abbreviated suffix that identifies the type of intermediary. For instance, 'abc.brk' will be adopted by stockbrokers, where 'abc' will be the chosen username and 'brk' denotes that the UPI holder is a stockbroker.

c) While an intermediary is free to use the same username across different banks, the suffix for each bank will be unique, to form a unique UPI ID.

d) These UPI IDs will also include a unique identifier handle '@valid' – along with the name of the self-certified syndicate bank as set out in the SEBI Circular. These handles will be allocated by NPCI exclusively for payment collection by SEBI-registered intermediaries.

2. **Additional security measures**: For investors to easily identify authenticated payments to registered intermediaries, a distinctive icon (i.e., "*white thumbs-up inside a green triangle*") will appear once a payment is initiated using the validated UPI handle. If the icon is not visible, investors will be alerted that the UPI handle is not validated. Investors are cautioned not to proceed with the transaction in such case. Intermediaries will also be required to generate 'QR' codes that prominently display this 'thumbs-up' logo.

3. **'SEBI Check' tool**: Additionally, SEBI is also introducing a digital tool called 'SEBI Check' for an added layer of security and verification. This tool will allow investors to carry out real-time verification as follows:

a) verify UPI IDs: Investors can verify the legitimacy of a UPI ID either by scanning a QR code provided by the intermediary or by manually entering the UPI ID; and

b) confirm bank details: The tool will retrieve and display the associated bank details (for example, the bank account number and Indian Financial System Code), allowing investors to confirm that the UPI ID belongs to a registered intermediary.

Purpose and benefits

1. **Mandatory requirement to obtain UPI IDs**: While for an investor, it is optional to make a payment though the UPI mechanism, it is mandatory for SEBI registered intermediaries to obtain unique UPI IDs and provide such option to the investor.

2. **Enhanced investor protection**: The verification methods enable investors to confirm the authenticity of a payment recipient and mitigate instances of fraud.

3. **Transaction limits**: Payments of up to INR 5,00,000 (Indian Rupees five lakh) per day *via* UPI will be available for capital market transactions supporting large investments without compromising security.

4. **Visible and easy verification**: The integration of the 'thumbs-up' icon and the use of QR codes in supporting this security framework simplifies the process of verification for investors.

Implementation/transition process

The utility developed to create UPI IDs and QR code will be made available on SEBI intermediary Portal ("**SI Portal**"). In this regard, certain key elements of the implementation/transition process are set out below.

1. **In terms of the investor**: Both the 'Validated UPI Handles' and the 'SEBI Check' tool will be available for use by investors and mandatory for intermediaries from October 1, 2025. While new fund transfers and new Systematic Investment Plans ("**SIPs**") will need to adhere to the new UPI ID structure from this date, existing ongoing SIPs will continue to function with their current UPI IDs for a transition period to avoid disruption.

2. **In terms of investor-facing intermediaries**: The intermediaries are required to comply with certain requirements as part of the implementation/transition process, including:

a) ensuring that their mobile number and email address are updated in the SI Portal;

b) ensuring that they apply for and obtain new UPI IDs from the banks;

c) creating investor awareness about the new payment handles and 'SEBI Check' function

through modes such as SMS, email, social media posts, audio visual messages, displays on website;

d) creating awareness and educational content for investors by placing relevant frequently asked questions on the respective websites; and

e) to stop accepting payments from other UPI handles post the specified deadline aside from existing SIPs.

3. **In terms of self-certified syndicate banks**: The banks are required to obtain application programming interface access to the SI Portal to issue the unique UPI IDs post verification and diligence.

Conclusion

SEBI's proactive efforts in introducing real-time verification tools and secure UPI payment mechanisms are aimed at reducing impersonation and increasing payment transparency. Given that existing systems of NPCI and banks are already in place to issue UPI handles, this provides an economical solution for an otherwise large issue. Further, the transition process is relatively straightforward for intermediaries, as it is routed through SI Portal) and the new UPI handles will be linked to existing bank account of such intermediaries. As such, the framework under the SEBI Circular highlights SEBI's commitment to provide a safe payment ecosystem for investors while promoting ease of investor participation in the securities market.

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

Ministry of Electronics and Information Technology

Ministry of Electronics and Information Technology releases blueprint for consent management

As India moves toward implementing the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), a key focus area has been developing robust frameworks for user consent management. In this context, the National e-Governance Division under the Ministry of Electronics and Information Technology ("**MeitY**"), has published a Business Requirement Document ("**BRD**") for consent management.

The BRD is a non-binding technical reference issued by MeitY's Startup Hub and is not part of the DPDP Act. The BRD was published as part of an Innovation Challenge, inviting participants to build a prototype Consent Management System ("**CMS**"). It is accessible on the MeitY Startup Hub website *here*. While the document is not intended to serve as official guidance under the DPDP Act, it does, however, serve as an early indication of how the Government may be thinking about consent architecture.

Regulatory context

The DPDP Act is currently not enforceable. The Government released the Draft Digital Personal Data Protection Rules, 2025, in January 2025, to operationalise the law. These draft rules address procedures and technical standards for compliance, including obligations around security, notices, and breach notifications. The public consultation period closed in March 2025, and final rules are awaited.

Key features of the BRD

The BRD lays out a modular, privacy-by-design CMS architecture, supporting the full consent lifecycle - collection, validation, renewal, withdrawal, and auditing. Some of the notable features include:

1. **Consent collection**: Consent is triggered when an individual initiates a service requiring personal data processing, such as account registration or onboarding. The CMS identifies the relevant processing purposes and generates consent requests accordingly. In this context:

   a) consent must be unbundled, granular, and purpose-specific, collected via explicit UI controls (e.g., toggles, checkboxes), with no pre-checked options;

   b) consent must be validated as free, specific, informed, unambiguous, explicit, and affirmatively given;

c) upon validation, the CMS generates a consent artefact containing key metadata (user ID, purpose ID, session ID, timestamp, consent method), which is securely stored in the consent database;

d) the system synchronises consent status across internal and external processors in real time via application programming interfaces; and

e) users receive an acknowledgement notification confirming submission, and all events are logged for auditability.

2. **Consent validation**: Before any data processing activity occurs, the CMS must validate the consent whether the required consent exists and remains active. Consent may be validated in the following manner:

a) when a data controller initiates a processing action or system query, the CMS checks its database for an active consent artefact matching the specified purpose and user ID;

b) consent must be current and not withdrawn or expired;

c) importantly, processing must remain within the scope of the consent provided. For instance, personal data collected for authentication cannot be reused for marketing without separate consent;

d) based on the outcome, the CMS either approves or denies processing. The user is notified of any denial; and

e) all validation actions are immutably logged to maintain a verifiable audit trail.

3. **Cookie consent**:

a) The cookie consent component ensures transparency and control over tracking technologies used on websites and apps, empowering users to make informed choices about their data.

b) On the first visit, a cookie banner must inform users of the use of cookies and similar technologies.

c) Users must be provided granular consent options across cookie categories such as essential, performance, analytics and marketing.

d) Only essential cookies may be enabled by default; all others require explicit, opt-in consent.

e) The CMS must offer a dedicated cookie preference interface where users can modify or withdraw consent at any time, with preferences updated in real time.

4. **Grievance redressal**: The BRD outlines a comprehensive redressal system as described below, that allows individuals to raise complaints related to data processing, privacy violations, or consent issues:

a) complaints will be automatically categorised (e.g., consent violation, data breach, processing error) and assigned unique reference IDs;

b) acknowledgement notifications will be sent upon submission, and all complaint data (user ID, timestamp, complaint type, and description) will be securely transmitted using TLS 1.3 (one point three) encryption;

c) a real-time resolution tracking dashboard will display complaint status (e.g., submitted, in progress, resolved), with updates and outcome notifications issued to the user; and

d) an escalation workflow will auto-forward unresolved complaints to the data protection officer if not closed within specified timeframes.

Conclusion

The BRD offers a preview of the operational contours of consent management under India's evolving data protection regime. While non-binding, it can help organisations future-proof their systems and prepare for robust, compliant consent workflows.

Quick Snapshots

1. **RBI proposes to introduce exclusive domain names**: With an aim to curb fraud in digital payments, RBI has introduced an exclusive internet domain name (bank.in) for Indian banks. RBI is yet to issue detailed guidelines in relation to such allocation. However, RBI has clarified that the Institute for Development and Research in Banking Technology will act as the exclusive registrar for these domain names. Going forward, RBI also proposes to introduce an exclusive domain name "fin.in" for other non-bank entities in the financial sector. This initiative will reduce cyber security threats and malicious activities like phishing and streamline secure financial services, thereby enhancing trust in digital banking and payment services.

2. **RBI proposes to enhances transaction limits in UPI**: Under the Statement on Developmental and Regulatory Policies, RBI has proposed to enhance UPI transaction limits beyond the current cap of INR 1,00,000 (Indian Rupees one lakh) (approx. USD 1,170 (US Dollars one thousand one hundred and seventy)). RBI has, however, clarified that the cap for peer-to-peer transactions will continue to be INR 1,00,000 (Indian Rupees one lakh) (approx. USD 1,170 (US Dollars one thousand one hundred and seventy)) and further, that banks will continue to have the discretion to decide their own internal limits within these revised limits.

3. **RBI instructs REs to route all applications through the PRAVAAH portal**: With an aim to achieve end-to-end digitisation of all internal workflows involved in the regulatory approval process, RBI launched the PRAVAAH portal on May 28, 2024. With effect from May 1, 2025, RBI has instructed all applicants, including REs to use the PRAVAAH portal to submit all applications for regulatory authorisations, licenses and approvals. While applicant are permitted to submit applications directly in exceptional situations, RBI has clarified that even such applications, once submitted, will be processed through the PRAVAAH system.

4. **NPCI plans to stop pull transactions**: In line with the Government's broader vision of securing digital payments, NPCI is moving towards curbing online payment frauds by phasing out collect calls for merchant transactions. To this end, NPCI has requested payment aggregators and banks to authenticate big merchants before allowing them to use collect calls. However, guidelines for implementing this are yet to be released.

5. **FinTechs come together to establish a new SRO**: Members of the FinTech Convergence Council, including prominent FinTech founders, including those behind Jupiter, Fi and Lendingkart, have come together to establish the India Fintech Foundation, a newly proposed SRO for the FinTech sector. They await approval from RBI to function as an SRO. The organisation is proposed to be a representative of the entire FinTech industry, from payments to lending to digital currency. At present, RBI has recognised the Fintech Association for Consumer Empowerment as an SRO in the FinTech sector.

6. **RBI approves new Payment Aggregator licenses**: RBI has granted Payment Aggregator ("**PA**") licenses to several PAs, including Easebuzz Private Limited (Easebuzz), Nomisma Mobile Solutions Private Limited (ftcash), Phi Commerce Private Limited (Payphi), Resilient Payments Private Limited (BharatPe X) and Vay Network Services Private Limited (VendorToPay).

7. **RBI directs Non-Banking Financial Companies not to factor in fintech guarantees while calculating loan provisions**: With an aim to reduce systemic risks and encourage sound credit practice, RBI has directed Non-Banking Financial Companies ("**NBFCs**") to exclude DLGs provided by fintech partners while provisioning for bad loans. As a result, DLG-backed loans will now be treated as unsecured loans, requiring higher provisioning and reduce net margins. This move could have a significant impact on loans originated through fintech companies acting as LSPs, since this requirement will increase the credit risk associated with such loans. The move also forces NBFCs to set aside higher amounts, potentially reducing capital availability and slowing digital lending growth. This communication from RBI is a setback for fintech startups that act as LSPs for NBFCs, supporting their lending services.

8. **RBI introduces 'theme neutral' and 'on tap' model for its regulatory sandbox framework**: RBI has proposed to introduce a 'theme neutral' and 'on tap' model for its regulatory sandbox. Earlier, under the regulatory sandbox, RBI would

introduce themes and specific window for applying within such themes. However, introduction of a 'theme neutral' and 'on tap' model would mean eligible entities will be able to submit proposals for testing any innovative product or solution within the RBI's regulatory ambit, without waiting for a specific theme or window. The move is aimed at fostering continuous innovation and deeper engagement with the fintech ecosystem.

9. **RBI approves new online PA and PA-Cross Border**: RBI has granted PA licenses to several PAs, including Hiveloop Internet Private Limited, Khatabook Technologies Private Limited, PayU Payments Private Limited, Pine Labs Private Limited and Zaak ePayment Services Private Limited. Additionally, RBI has also authorised Worldline ePayments India Private Limited to operate as an export and import PA-Cross Border ("**PA-CB**") and granted PayPal Payments Private Limited, the Indian subsidiary of PayPal Holdings Inc., an in-principle authorisation to operate as a PA-CB.

10. **NPCI reiterates the requirement to display the name of the ultimate beneficiary**: NPCI has reiterated the requirement for UPI apps to display only the ultimate beneficiary's name (as per the core banking system) for all transactions. This move is intended to instill confidence in users that they are sending money to the correct beneficiary and to avoid potential risk of fraud.

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

Nand Gopal Anand
Partner

Abhishek Ray
Partner

Pulkit Sukhramani
Partner

Yajas Setlur
Partner

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

12 Practices and 50 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Recognised in World's 100 best competition practices of 2025

Among Best Overall

Law Firms in India and

14 Ranked Practices

---

9 winning Deals in

IBLJ Deals of the Year

---

11 A List Lawyers in

IBLJ A-List - 2025

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm
of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services
Law Firm of the Year 2022

Ranked Among Top 5 Law Firms in India for ESG Practice

2022

Ranked #1
Best Law Firms to Work

Top 10 Best Law Firms for Women

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

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