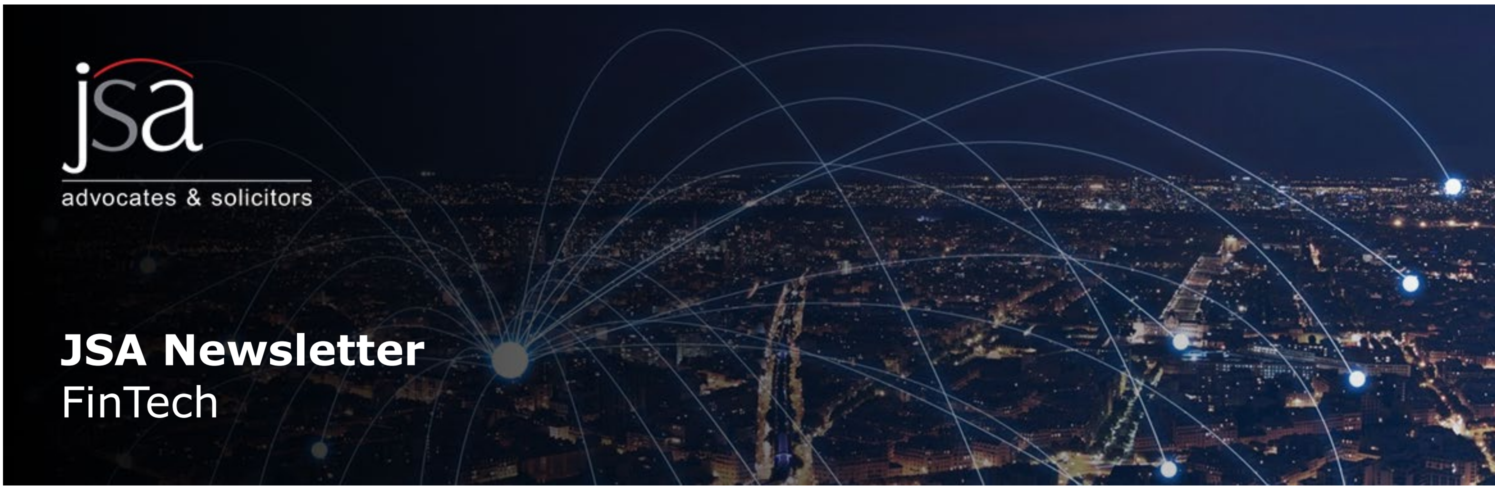

jsa
advocates & solicitors

JSA Newsletter
FinTech

Twelfth Edition, 2021

# RBI Issues PSO Outsourcing Framework

## RBI issues Outsourcing Framework to mitigate risks and enforce minimum security controls

On August 3, 2021, the Reserve Bank of India ("**RBI**") issued a Framework for Outsourcing of Payment and Settlement-related activities by payment system operators ("**Outsourcing Framework**"). According to RBI's observations, non-bank payment system operators outsource the majority of their payment and settlement-related activities to third parties. In the absence of a uniform framework to regulate such outsourced activities, they are exposed to several plausible risks and security threats. To mitigate attendant risks in outsourcing payment and settlement related activities by non-bank payment system operators ("**PSOs**"), and to enforce minimum security controls, RBI has issued the Outsourcing Framework. The Outsourcing Framework applies to non-bank PSOs only to the extent of their payment and settlement related activities. The salient features of the Outsourcing Framework include:

1. **No prior approval from RBI**: Outsourcing payment and settlement related activities by PSOs under this Outsourcing Framework does not require RBI's prior approval.

2. **Scope of third party service providers**: Payment and settlement related activities can be outsourced to 'service providers' which include, but are not limited to, vendors, payment gateways, agents, consultants and / or their representatives that are engaged in the activity of payment and / or settlement systems, sub-contractors (i.e., secondary service providers) to whom primary service providers may further outsource whole or part of some activity related to payment and settlement system activities outsourced by the PSOs (whether located in India or outside). The selection of service providers will be based on comprehensive risk assessment undertaken by PSOs.

3. **Bar on outsourcing core management functions**: PSOs will not outsource core management functions, including risk management and internal audit; compliance and decision-making functions such as determining compliance with KYC norms. 'Core management functions' include but are not limited to, management of payment system operations (netting, settlement, etc.); transaction management (reconciliation, reporting and item processing); granting sanction to merchants for acquiring; managing customer data; risk management; information technology & information security management etc.

4. **Limitation on ownership/control of the service provider**: Service providers, except for group companies of PSOs, will not be owned or controlled by any director or officer of the PSOs or their relatives (the terms – control, director, officer and relative will have the same meaning as assigned to them under the Companies Act, 2013).

5. **Due diligence and risk management**: Since outsourcing activities can be met with various risks, PSOs must exercise due diligence, put in place sound and responsive risk management practices for effective oversight, and manage risks arising from such outsourcing of activities.

6. **PSOs' own obligations**:

(i) Outsourcing of any activity by PSOs will not reduce their own obligations, obligations of their boards and senior management, and they will be liable for the actions of its service providers. PSOs should retain ultimate control over their outsourced activities.

(ii) Outsourcing activities will not affect rights of customers against PSOs, including their ability to avail grievance redressal as applicable under the relevant laws. Responsibility of addressing grievances of customers will vest with PSOs, including in respect of the services provided by the outsourced agency (i.e., service provider).

(iii) If PSOs have outsourced their customer grievance redressal function, they must also provide customers with the option of direct access to their nodal officials for raising and / or escalating complaints. Such access should be enabled through adequate phone numbers, e-mail ids, postal address, etc., details of which will be displayed prominently on their websites, mobile applications, advertisements, etc., and adequate awareness must also be created about the availability of this recourse.

7. **Monitoring by PSOs**:

   (i) PSOs must regularly review and monitor the security practices and control processes of their service providers and require such service providers to disclose security breaches. The PSOs will immediately notify the RBI about any breach of security and leakage of confidential information related to customers. In the event of a breach of security or leakage of confidential information, the PSO would stand liable to its customers for any damage.

   (ii) PSOs must ensure that their service providers (domestic or off-shore) follow the extant instructions related to storage of payment system data.

8. **Isolation of PSOs' documents**: PSOs must ensure that their information, documents and records, and other assets are isolable by their service provider. This is to enable PSOs, in appropriate situations, to remove from the possession of the service providers, information, documents and records with regard to the PSOs' outsourced activities; delete/destroy such records or render them unusable.

9. **Off-shore Outsourcing**: Since engagement of a service provider in a foreign country exposes PSOs to country risk, in order to manage such country risk, PSOs must closely monitor government policies and, political, social, economic and legal conditions in countries where the service provider is based, both during the risk assessment process and on a continuous basis and establish sound procedures for dealing with country risk problems. This includes having appropriate contingency and exit strategies.

# RBI Issues New Master Directions on PPIs

## RBI's new Master Directions on prepaid payment instruments introduces new classifications and perpetual validity for authorization

On August 27, 2021, RBI issued the Master Directions on Prepaid Payment Instruments, 2021 ("**PPI Master Directions**"). The PPI Master Directions have been introduced with an aim to achieve interoperability of prepaid payment instruments ("**PPIs**") and to regulate issuers of such PPIs.. Some of the key changes introduced under these PPI Master Directions have been discussed below:

1. **New Classification of PPIs**: PPIs have been classified into two broad categories of (a) Minimum-detail PPI (also known as "**Small PPI**"); and (b) Full-KYC PPI.

   As the name suggests, Small PPIs require minimum details of the PPI holder, *viz*. a mobile number verified with OTP ; a self-declaration of the PPI holder's name; and unique identity / identification number of any 'mandatory document' or 'officially valid document'. Small PPIs can be used for purchase of goods and services and exclude cash withdrawal and fund transfer.

   Small PPIs have been distinguished into two types, i.e. Small PPI (with cash loading facility) and Small PPI (without cash loading facility).

The key difference between the two types is that a Small PPI (with cash loading facility) can be loaded/reloaded using cash, whereas, a Small PPI (without cash loading facility) can only be loaded/reloaded using a bank account, credit card or full-KYC PPI (excluding cash).

Full KYC PPIs, on the other hand, require completion of KYC of the PPI holder and can be used for cash withdrawal and fund transfer, in addition to their use for purchasing goods and products. Under the new PPI Master Directions, a Full KYC PPI can be issued even by non-banks, which was not allowed for Open system PPIs under the erstwhile PPI framework.

2. **Validity for Certificate of Authorisation ("CoA")**: The CoA will be granted for perpetuity under the new PPI Master Directions. This is a better position as validity for a CoA was only for 5 years under the earlier framework.
3. **Interoperability**: Under the new PPI Master Directions, PPIs will have to (a) mandatorily implement interoperability for full-KYC PPIs via authorised card networks (for card-based PPIs) and UPI (for wallets). Interoperability is optional for Gift PPIs and exempted for PPIs issued for mass transit systems.
4. **Enhancement of Maximum Limits for Full KYC PPIs**: Under the new PPI Master Directions, the RBI has increased the maximum amount outstanding in respect of Full-KYC PPIs from INR 1 lakh to INR 2 lakhs.
5. **Introduction of a Cooling Period**: A mandatory 'cooling period' of 1 year has been introduced which would apply to the following entities in the given situations:

   (i) Authorised payment system operators (including PPI issuers) whose authorisation has been revoked or not renewed by the RBI;

   (ii) Authorised PSO that has voluntarily surrendered its authorisation;

   (iii) An entity whose application for authorisation as a PSO has been rejected by the RBI;

   (iv) Any new entity setup by the promoters of the entities mentioned in (a), (b) or (c) above.

   Therefore, an entity to which any of the above given conditions apply would be prohibited from submitting an application to the RBI for authorization to act as a PSO/PPI issuer during the 1-year cooling period.
6. **Miscellaneous**:

   (i) Introduction of Two Factor Authentication: PPIs are required to implement a 'Two Factor Authentication' ("**2FA**") for all wallet transactions involving debit to wallet transactions and cash withdrawals.

   (ii) Gift Instruments: Cash-out or funds transfer are not permitted for gift instruments. However, transfer of funds back to the source account has been allowed subject to the PPI holder's consent.

   (iii) Cross Border Transactions: Under the earlier framework, cross border transactions in INR denominated PPIs could be carried out by way of KYC compliant semi-closed PPIs and open PPIs issued by AD-1 banks. However, under the new PPI Master Directions, such issuances can only be done via Full-KYC PPIs issued by AD-1 banks. Other conditions for cross border transactions have not been altered.

# RBI Updates Tokenisation Framework

## RBI's latest circular on tokenization extends tokenization to Card-on File Tokenisation and now allows card issuers to offer tokenization services

On January 8, 2019, the RBI permitted authorised card payment networks ("**Card Networks**") to offer card tokenisation services to third-party app providers ("**Token Requestors**"). The RBI allowed Card Networks to offer tokenisation for all use cases, including near field communication (NFC) / magnetic secure transmission (MST) based contactless transactions, in-app payments, and QR code-based payments. However, Card Networks were only allowed to enable tokenisation through trusted devices – originally, mobile phones and tablets and more recently, IoT devices and wearables. This means that any 'token' issued by a Card Network in place of actual card details must be linked to a specific device.

Stakeholders in the payments industry  had repeatedly urged the RBI to create a more permissive tokenisation framework that looks beyond device-based tokenisation. Merchants, payment intermediaries and industry bodies have requested the regulator to allow cloud-based tokenisation, a mechanism whereby customers and merchants can create and retrieve tokens regardless of the device used by the consumer to initiate payment transactions.

In 2021, the RBI permitted card-on file tokenisation ("**CoFT**") in its circular dated September 7, 2021 ("**CoFT Circular**"). Some of the notable features of the CoFT Circular have been summarised below:

1. **Cloud-based Tokenisation**: While the RBI's existing tokenisation framework relies on trusted-devices, i.e., mobile phones, tablets etc., the new framework allows for cloud-based tokenisation, whereby tokens are not linked to a particular device. This marks a significant and positive departure from the existing regulatory framework. Several stakeholders, particularly e-commerce merchants, have complained since 2019 that device-based tokenisation would be unfeasible to practically implement and is an inadequate substitute for actual card-on-file data.

2. **Issuers permitted to Tokenize**: The RBI's CoFT Circular permit issuing banks to provide tokenisation services (in addition to Card Networks) and to act as token service providers ("**TSPs**"). Such TSPs are permitted to offer tokenisation services only for cards issued by or affiliated with them and are responsible for ensuring compliance with the framework.

   However, it remains to be seen how issuing banks would practically enable CoFT on a large scale. In practice, merchants may prefer utilizing the tokenisation services of Card Networks, so as to avoid separately engaging/contracting with multiple issuing banks.

3. **Streamlined AFA**: The requirement for additional factor of authentication ("**AFA**") continues to apply to tokenisation under the updated framework. However, the RBI has clarified that AFA validation may be combined and undertaken simultaneously where a card payment transaction and a registration for CoFT are performed at the same time. This would come as a relief for e-commerce merchants who had complained of the friction caused by the multiple AFA validations mandated under the RBI's previous framework.

4. **Tokenisation not Mandatory**: Notably, the RBI has not made it mandatory for issuing banks to offer CoFT to their customers. Several merchants had hoped that the regulator would make tokenisation mandatory since long-tail banks are expected to take an inordinate amount of time to implement any form of tokenisation.

5. **Restrictions on Data Storage**: The RBI has taken this opportunity to reiterate its stance on card data storage, and has made it clear that tokenisation is the only RBI-approved solution for merchants to facilitate speedy payments. As per the CoFT Circular, no entity in the card transaction / payment chain, other than TSPs, are permitted to store any card data with effect from January 01, 2022. Most notably, the RBI has directed all such entities to delete data previous stored from their systems.

   This requirement to purge or delete card data is important and should be noted by any e-commerce company that proposes to house such data in card vaults or similar systems hosted by affiliate and third party entities.

6. **Clarity on "Limited Data"**: As an exception to the above restrictions, the RBI has clarified that non-TSP entities may continue to store (a) the last four digits of the actual card number; and (b) the card issuer's name ("**Limited Data**") for transaction tracking and/or reconciliation purposes.

   While merchants and fintech companies had craved for further clarity on the scope of Limited Data (since the RBI's clarifications in the PA/PG Guidelines), the RBI's definition appears much narrower than what most stakeholders may have hoped for. This statement may take companies back to the drawing board and may need them to re-evaluate their mechanisms for payment tracking and transaction fulfilment.

# NPCI Issues Merchant Acquisition Standards for Acquiring Member Banks

## The NPCI's Merchant Acquisition Standards are intended to hold Acquiring Member Banks accountable and liable for the merchants onboarded by them or through aggregators/third parties

On 8th September, 2021, vide circular NPCI/UPI/Rupay/OC-118/2021-22, NPCI has issued extensive guidelines that Acquiring Member Banks will be required to comply with at the time of onboarding merchants ("**Onboarding Guidelines**").

These Onboarding Guidelines (i) provide for a wide and inclusive definition of the word 'Merchant' which includes merchant, aggregator, marketplace, master-merchant and sub-merchant; and (ii) are intended to hold the Acquiring Member Banks fully accountable and liable for their merchants (whether onboarded directly by them or through aggregators/third parties). Acquiring Member Banks have been instructed to onboard merchants only after completion of due diligence on such merchants. As per the Onboarding Guidelines, Acquiring Member Banks require to have/conduct:

1. **Board approved policy for Merchant acquisition**: The Acquiring Member Banks need to have board approved policies providing for merchant acquisition standards and risk mitigation measures in respect of merchant onboarding.

2. **Agreements with various stakeholders**: Acquiring Member Banks should have in place executed agreements with each merchant that they onboard, including agreements with aggregators, third party service providers who onboard merchants on behalf of the Acquiring Member Banks.

3. **Merchant underwriting**: Acquiring Member Banks are required to conduct due diligence and checks with respect to merchants prior to their onboarding. Such due diligence will include but not be limited to verifying the merchant in relation to its origin country, ownership by foreign stakeholders in such entity and its mobile application.

4. **Merchant portfolio and risk monitoring**: Acquiring Member Banks will be required to monitor the activities, sales, portfolio of its merchants and take legal action for any fraudulent/illegal acts done by such merchants.

5. **Merchant training**: Acquiring Member Banks should impart training to its merchants and prepare modules/FAQs periodically.

6. **Third party agent risk oversight and governance**: Acquiring Member Banks will conduct periodic audits of any third parties engaged by merchants and remain responsible for any security related activities outsourced to such third parties.

# NPCI Introduces Numeric ID Mapper

## In order to create a 'simple' payment address, the NPCI has introduced a Numeric UPI ID (referred to as "UPI Number") for transaction routing

The NPCI has introduced a Numeric ID Mapper, referred to as UPI Number, which will be mapped against the respective UPI ID of a customer and resolve mapping to the respective PSP/TPAP for transaction routing. This will be a simpler option for customers instead of the existing alphanumeric UPI ID ('Username@PSP').

While a few PSPs / TPAPs have been using mobile numbers as an alias to UPI IDs for P2P and P2M payments using UPI apps, customers do not experience interoperability between PSPs / TPAPs, which the NPCI seeks to implement through this circular.

Customers will have a choice of 8 to 11 digits for their UPI Number, however in case of 10 digit UPI numbers the customer will only be allowed to set their own mobile number. The generation of UPI Number is voluntary and is based on explicit user consent. Customers have the choice to have multiple UPI Numbers for different app providers, but where the mobile number is used as the UPI Number, the same can only be linked to a single UPI ID, at any instance.

## Quick Snapshots

### 1. India and Singapore announce linkage of their Fast Payment Systems

On September 14, 2021, RBI and the Monetary Authority of Singapore ("**MAS**") announced a project to link their respective countries' fast payment systems viz. Unified Payments Interface (UPI) of India and PayNow of Singapore. This linkage is targeted to come into operation by July 2022.

This linkage will allow users of each of the two fast payment systems to make instant, low-cost fund transfers on a reciprocal basis and does away with the need to get onboarded onto the other payment system as a pre-requisite. This initiative will provide a huge impetus to trade between India and Singapore by significantly reducing time and charges in making cross border payments.

### 2. NPCI mandates enablement of international payments on UPI

On September 8, 2021, through circular NPCI/UPI/OC – 117/2021-22, NPCI has mandated Member Banks, TPAPs and other payment providers on UPI to enable international merchant payments on UPI as a mandatory feature by December 31, 2021. International merchant payments were introduced in UPI in September 2020 and are already live in Singapore and Bhutan. The NPCI aims to enable this in other countries in the coming months.

### 3. RBI allows Aadhaar e-KYC by non-banks

On September 13, 2021, the RBI issued a notification enabling entities, other than banking companies, to be permitted to carry out authentication of clients' Aadhaar numbers using e-KYC facility provided by UIDAI. Non-banking Finance Companies, Payment System Providers and Payment System Participants may submit their applications to do so to the RBI for onward submission to UIDAI.

### 4. RBI sets fraud as the theme for the Fourth Cohort under Regulatory Sandbox

The RBI has selected 'Prevention and Mitigation of Financial Frauds' as the theme for the Fourth Cohort under Regulatory Sandbox. The RBI hopes for fintechs to play a pivotal role in strengthening fraud governance, reducing response time to frauds and the lag between occurrence and detection of financial frauds. The RBI's aim is to safeguard consumer interests and minimize losses from such frauds.

The Regulatory Sandbox is a formal regulatory programme for market participants to test new products, services or business models with customers in a live environment, subject to safeguards and oversight by the RBI to provide regulatory guidance.

### 5. RBI amends Master Direction on Account Aggregators

On October 5, 2021, the RBI amended the Master Direction on Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, prohibiting new investors from or through non-compliant FATF jurisdictions from directly or indirectly acquiring 'significant influence' in existing NBFC-AAs (account aggregating NBFCs) or companies seeking Certificate or Registration for the same. However, investors in existing NBFC-AAs holding their investments prior to the classification of the source or intermediate jurisdictions as FATF non-compliant may continue with the investments or bring in additional investments so as to support continuity of business in India.

The October 5 amendment also includes additional requirements for NBFC AAs to comply with to declare dividends from the profits of the financial year ending March 31, 2022 onwards, including meeting the prescribed leverage ratio in each of the last 3 financial years including the financial year in which the dividend is proposed.

## 6. Investments in Fintech Sector

- Full-stack financial services platform, WeRize has raised USD 8 million in its Series A funding round led by 3one4 Capital, Kalaari Capital, Orios Ventures and Picus Capital.
- NFTically, a global platform for buying and selling of non-fungible tokens has been launched with seed funding from Matic Network CEO, Jayanti Kanani.
- Prosus, along with fintech subsidiary PayU, have announced the signing of their agreement to buy payment gateway service provided BillDesk for USD 4.7 billion. The transaction is subject to approval by the Competition Commission of India.
- Fintech platform Khatabook has raised USD 100 million in Series C investment led by Tribe Capital and Moore Strategic Ventures. Other investors include Sequoia Capital, Alkeon Capital, B Capital Group, Tencent, RTP Ventures, Better Capital and Unilever Ventures. Operated by ADJ Utility Apps based in Bangalore, Khatabook's valuation is now USD 600 million.
- Online lending and financial services provider True Balance has raised USD 15 in debt funding for its lending arm, True Credits. The capital has been raised from Pace Group and E-clear, among other Korea based investors.
- Klub, a revenue-based financing platform, has raised USD 20 million in a seed round from 9Unicorns and Sequoia Capital India's Surge, along with Alter Global and GMO Venture Partners.
- InCred Financial Services Ltd, based out of Mumbai, has closed its second issue of covered bond for INR 75 crore (USD 10 million). Investors included family offices, ultra HNIs, corporate treasuries and NBFCs.
- Cross-border remittance API provider Nium is now valued at above USD 1 billion after having raised over USD 200 million in a Series D round. The round was led by Riverwood Capital, a venture capital firm based out of California. Temasek, Vertex Ventures, Visa, Beacon Venture Capital, Atinum Group of Funds, Rocket Capital Investment, and other angel investors also participated in this round.

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

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

This update is not an advertisement or any form of solicitation and should not be construed as such. This update has been prepared for general information purposes only. Nothing in this update constitutes professional advice or a legal opinion. You should obtain appropriate professional advice before making any business, legal or other decisions. JSA and the authors of this update disclaim all and any liability to any person who takes any decision based on this publication.