RBI Framework for Outsourcing of Payment and Settlement Activities by Non-Bank Payment System Operators

02 September 2021

This update covers:

On 3 August 2021, the Reserve Bank of India (**RBI**) issued the '*Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators*' (**Framework**), under the Payment and Settlement Systems Act, 2007 (**PSSA**). The Framework regulates certain outsourcing activities by non-bank payment system operators (**PSOs**). While certain banks are also authorised to act as PSOs, the Framework only applies to non-bank PSOs since banks and non-banking financial companies are already subject to similar requirements in relation to the outsourcing of their financial service activities.

The RBI has released a new framework governing the outsourcing of activities by non-bank payment system operators. In this update we summarize the salient features of this framework and its implications.

A 'payment system' is *a system that enables clearing, payment or settlement (or all of them) between a payer and a beneficiary and includes systems enabling operations relating to credit, debit and smart cards, money transfer and other similar activities but does not include a stock exchange*. Examples of such payment systems include digital wallets like PayTm and Mobikwik, card payments networks like MasterCard and American Express, Unified Payments Interface (**UPI**) etc.

The term 'outsourcing' is defined as the use of a third party to perform activities on a continuing basis, including short term arrangements, that would normally be undertaken by the PSO itself. Therefore, apart from the vendor, the Framework also applies to agents, consultants and their representatives, as well as sub-contractors engaged by the vendor, whether or not located in India. Such outsourcing is very common in the financial services sector.

Additionally, the RBI has observed in the Framework that it would be prudent for payment system participants such as third-party UPI application providers, token requestors etc. which are not directly regulated or supervised by the RBI but may be providing direct payment services to customers to implement a system to manage outsourcing risks. As a best practice, the RBI has therefore recommended that PSOs may engage with such payment participants to encourage them to implement the Framework. Consequently, it seems likely that PSOs may seek to contractually require participants in their payment systems to implement the Framework. The Framework's release comes in light of recent cyber-attacks that targeted customer data in the possession of certain PSOs as a result of which large amounts of information was allegedly leaked. The Framework seeks to manage the risks to PSOs which may arise from vulnerabilities in the systems of vendors.

1 Scope of the Framework

The Framework covers outsourcing of payment and/or settlement related activities of PSOs, i.e., the processes in a payment system which enable the transfer of funds from the payer to the payee. Payment gateways, tokenisation solutions, application hosting, KYC verification, payment reconciliation etc. are also covered.

Additionally, the Framework applies to incidental activities such as the onboarding of customers and IT support services. Activities that are not related to payment or settlement services such as internal administration, house-keeping and similar activities are explicitly excluded from the Framework.

2 Core management functions and critical processes

The Framework restricts PSOs from outsourcing their core management functions, including risk management and internal audit, compliance and decision-making functions such as determining compliance with KYC norms. A similar restriction also applies to banks and NBFCs. However, the Framework takes it one step further and specifies that the following additional core management functions will be restricted: (i) management of payment system operations such as netting, settlement, etc.; (ii) transaction management (reconciliation, reporting and item processing); (iii) sanctioning merchants for acquiring or managing customer data; (iv) risk management; (v) information technology (IT) and information security (IS) management.

Many PSOs currently do not have the means and/or resources to invest in the sophisticated systems necessary for carrying on activities like transaction and risk management handling of customer data. and extensive IT and IS functions. Similarly, while PSOs may have capacity for undertaking IT/ IS functions, PSOs often opt to outsource these functions in order to focus on their core business. They usually engage specialized vendors who provide the necessary platforms or infrastructure as services to the PSOs at significantly lesser costs. However, outsourcing of such functions could result in increased cyber security threats since a fault on the vendor's systems could potentially expose all PSOs relying on the services of such vendor and affect millions of customers. This seems to be the intent behind restricting such outsourcing.

While the Framework restricts outsourcing of core management functions, it allows PSOs to outsource their 'critical processes' after evaluating the need for such outsourcing and the selection of vendors, based on a comprehensive risk assessment. Critical processes are those which,if disrupted, will have the potential to significantly impact the PSOs' business operations, reputation, profitability and / or customer service. There is

a possibility that such processes may overlap with the PSOs core management functions and the Framework should ideally have provided further guidance to help distinguish the two categories.

3 Arrangements with group companies

A PSO may outsource functions to its group companies subject to its board approved policy. The arrangement needs to be documented as a written agreement setting out the service levels to be met by the group entity, service charges to be paid by the PSO, confidentiality obligations on the group entity in respect of customer data etc. The PSO must also ensure that the agreement with the group entity does not prevent the RBI from obtaining any information required for the supervision of the PSO, or pertaining to the group as a whole. Current outsourcing arrangements between PSOs and their group entities may need to be re-examined in light of these restrictions.

The Framework also stipulates certain conditions for cross-selling by PSO and group entities with the intent to ensure that customers are informed of which entity actually provides the services. The PSO must not give the impression that it is responsible for the obligations of the group entities. Additionally, the vendor must not be owned or controlled by any director or officer of the PSO or their relatives unless it is a group company of the PSO. This move appears to improve transparency in financial service offerings from PSOs.

4 Data

4.1 Customer data

As discussed above, the Framework restricts PSOs from outsourcing customer data management. This is commonly understood to mean the people, processes and technologies involved in collecting, classifying, cleaning, correcting and enriching data, and combining the data for analytics etc.

However, the Framework does not prohibit sharing of customer data with vendors since it expressly contemplates that customer data may be in the custody or possession of the vendor, though it prescribes some conditions that need to be adhered to. These include (i) ensuring that the vendor has the ability to isolate and clearly identify all customer information, documents, records, and assets, (ii) requiring that customer data belonging to each PSO is encrypted or otherwise adequately safeguarded by the vendor to protect customer confidentiality and prevent co-mingling of information, (iii) ensuring that vendor's staff accesses customer data only on a 'need-to-know' basis, (iv) conducting regular review and monitoring of the security practices and control processes of the vendor and (v) requiring the vendor to disclose security breaches to the PSO.

While the term 'customer data management' has a broad import, activities such as data hosting or analytics can be excluded from its scope and carried out by outsourced vendors if they do not involve any data management. This would be relevant in the context of PSOs that have moved such processes to third party cloud based applications.

Where customer data is shared with vendors, the Framework requires PSOs to notify the RBI immediately of any security breach or leak of customer data at the vendor's end. The PSOs will also be liable towards the customers for damages in such cases.

4.2 Payment system data

PSOs are subject to RBI's notification dated 6 April 2018 on Storage of Payment System Data (**Localisation Mandate**), which mandates the payment system data to be brought back to India within one business day or

24 hours of payment processing and that the entire data relating to payment systems be stored locally in India. Payment system data includes customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc.); payment sensitive data (customer and beneficiary account details); payment credentials (OTP, PIN, Passwords, etc.); and transaction data (originating and destination system information, transaction reference, timestamp, amount, etc.).

The Framework now explicitly requires that the vendor adhere to these restrictions, whether located offshore or in India. The PSOs were already passing on these obligations contractually to outsourcing vendors. Hence, in practice, there may not be any new compliances for PSOs or their vendors.

5 Responsibility for and supervision of outsourced activities

Under the Framework, a PSO and its board and senior management retain full responsibility for the outsourcing and are liable for the actions of the vendor. A PSO should therefore exercise due diligence while outsourcing and also retain ultimate control over the outsourcing.

In this regard, the Framework also prescribes certain internal controls such as a comprehensive board-approved outsourcing policy, robust internal audit systems for outsourcing, regular audits of risk management practices, a management structure to oversee and monitor the outsourcing, timely reconciliation between PSO and vendor in case of outsourcing of cash management functions etc. Additionally, a PSO is required to review a vendor's financial and operational conditions, at least on an annual basis.

Further, a PSO must ensure that vendors develop and regularly test business continuity and recovery procedures in respect of the outsourcing activities. A PSO also needs to retain the flexibility to take appropriate measures to ensure continuity of the outsourced activity. This could be by way of transitioning the outsourcing activity to other vendors, bringing the function in-house etc. The PSO will also need to ensure that its documents, information etc. in possession of the vendor can be isolated and removed or deleted, destroyed or rendered unusable. Such business continuity related provisions are very common in services outsourcing and should not raise any challenges for PSOs to include in their outsourcing contracts.

6 Rights of customers

PSOs need to take measures to ensure that the outsourcing does not affect the rights of customers or payment system participants (for example, banks) against the PSO. The PSO is also responsible for addressing customer grievances including in relation to services provided by vendors.

Where customer grievance redressal functions are outsourced, the PSO should give customers the option to directly raise/ escalate complaints with its nodal officers. PSOs must take measures to ensure customers are made aware of this option through advertisements, display of nodal officer details on their website, mobile application etc.

In case a customer is required to interface with a vendor to avail a PSO's services, the PSO needs to make a statement to this effect in its product literature, brochure and other marketing communication and clearly demarcate the role of the vendor. If the PSO's agreement with the vendor terminates, the PSO must give this due publicity to ensure that their customers stop dealing with the concerned vendor.

7 Off-shore outsourcing

PSOs may also engage overseas vendors for outsourcing, subject to the Localisation Mandate. In such cases, PSOs must consider the following factors: (i) government policies and the political, social, economic and legal conditions applicable to the vendor, (ii) whether local laws of the vendor generally uphold confidentiality clauses and agreements, (iii) whether the regulator in the applicable foreign jurisdiction may obstruct the arrangement or object to visits by the RBI or the PSO for audits, assessments, inspections, etc. on the vendor. Additionally, the PSO must have a contingency and exit strategy ready. It must also ensure that (i) foreign regulators cannot have access to PSO's data in India, and (ii) the foreign courts cannot exercise jurisdiction over the PSO's operations and activities outsourced to the vendor. These conditions are in line with the outsourcing norms applicable to banks and NBFCs.

8 Outsourcing Agreements

The Framework also enumerates certain key provisions which are to be incorporated in the outsourcing agreement between a PSO and a vendor. These include (i) clear definition of the outsourced activity and the applicable service and performance standards, (ii) provisions giving the PSO the right to access all information relevant to outsourcing, (iii) clauses enabling monitoring and audit of the vendor by the PSO, (iv) clauses on maintaining confidentiality of customer data (even after termination of the agreement), (iv) provisions assigning liability to the vendor for data breaches and (v) clauses on exit management.

The agreement should also incorporate the right of the RBI to access the PSO's documents, record of transactions, and other necessary information available with the vendor and to inspect the vendor, if need be. The agreement must also include a provision that the vendor must obtain prior consent from the PSO for further delegating any outsourced activity to sub-contractors.

To summarise, the Framework focuses on upholding customer interests by implementing measures such as controls over data and processing carried out by third party vendors in the payment industry. The Framework will also bolster data security and will be beneficial for the protection of customer data. That said, the Framework is likely to increase compliance costs on non-Bank PSOs by imposing norms which would require changes to their existing operations or arrangements before next financial year.

Further, though the Framework largely aligns the regulatory approach towards outsourcing by PSOs with existing norms for outsourcing by banks and NBFCs and fills the gap on regulation of outsourcing by PSOs, it also seems to expand the scope of core management activities in financial services. For instance, the Framework provides an illustrative list of such functions in comparison to the norms for banks and NBFCs. With this specification of core management activities, functions such as transaction, security and customer data management, netting and settlement functions get covered within the scope of core management activities. Since the Framework restricts PSOs from outsourcing their core management functions, this expansion in scope of core management activities is likely to hinder innovation in technology and growth of the outsourcing industry.