Technology Law Analysis

August 19, 2021

FIRST OF ITS KIND OUTSOURCING REGULATORY FRAMEWORK FOR PAYMENT SERVICE PROVIDERS

- First of its kind regulation for non-bank Payment Service Providers
- Limitations on outsourcing 'core management' functions
- Payment Service Providers to be held liable for outsourcing activities
- Offshore and domestic outsourcing arrangements to comply with the regulatory framework

BACKGROUND

The Reserve Bank of India ("**RBI**"), India's apex bank recently issued a regulatory framework ("**Framework**") to be implemented by non-bank payment system operators / providers ("**PSPs**") for the outsourcing of payment and settlement-related activities to third party service providers. PSPs have been provided with a timeline of until March 31, 2022 to ensure that their outsourcing arrangements comply with the Framework.

WHAT IS A PSP?

As per the Payment and Settlement Systems Act, 2007 ("**PSS Act**"), a "payment system" means a *"system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange"*.[1] Payment systems include systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. An entity that *operates* a payment system is considered a 'payment system operator' (PSO) or 'payment system provider' (PSP), which needs to be authorized by the RBI.

PSPs can include payment aggregators, e-wallet and gift instrument issuers, card issuers and networks, money transfer networks, ATM networks and National Payments Corporation of India (NPCI) that operates the Unified Payments Interface (UPI), a system for fund transfers between bank accounts via a mobile platform.

SCOPE OF THE FRAMEWORK

'Outsourcing' under the Framework means use of a third-party service provider to perform activities on a continuing basis that would normally be undertaken by the PSP. 'Service providers' include vendors, payment gateways (PGs), agents, consultants and their representatives engaged in payment and settlement systems activities, including sub-contractors or secondary service providers.

The Framework seeks to put in place minimum standards to manage risks involved in outsourcing of payment and settlement-related activities by PSPs, including incidental activities like on-boarding customers, IT services etc.[2] The Framework is applicable to outsourcing of functions by PSPs to service providers in India and overseas.

OUTSOURCING FUNCTIONS

The PSP should ensure that it exercises due diligence, implements appropriate risk management practices for oversight, and manages risks arising from the outsourcing of activities. Specifically, in terms of critical processes and activities, the Framework requires PSPs to first evaluate the need to outsource such functions based on a comprehensive risk assessment.

The outsourcing should not impede or interfere with the ability of the PSP to oversee and manage its activities, nor prevent the RBI from carrying out its supervisory functions. More importantly, the PSP shall continue to be held liable for the actions of its service providers.

OUTSOURCING RESTRICTIONS

The Framework *restricts* PSPs from outsourcing '*core management functions*' that include risk management, internal audit, compliance and decision-making functions such as determining KYC compliance. 'Core management functions' include management of the payment system operations, transaction management, according sanction to merchants for acquiring, managing customer data, risk management, information technology and information security management.

PSP COMPLIANCE FRAMEWORK

The Framework sets out a host of compliance obligations to be fulfilled by the PSP in outsourcing functions to service providers, broadly including the following:

1. Supervisory Functions: The PSP would be responsible for the outsourced activity and liable for the actions of its

Research Papers

Handbook on Labour Codes
April 29, 2024

Compendium of Research Papers
April 11, 2024

Third-Party Funding for Dispute Resolution in India
April 02, 2024

Research Articles

Private Client Insights - Sustainable Success: How Family Constitutions can Shape Corporate Governance, Business Succession and Familial Legacy
January 25, 2024

Private Equity and M&A in India: What to Expect in 2024?
January 23, 2024

Emerging Legal Issues with use of Generative AI
October 27, 2023

Audio

Third-Party Funding: India & the World
April 27, 2024

IBC allows automatic release of ED attachments: Bombay HC reaffirms
April 15, 2024

The Midnight Clause
February 29, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Cyber Incident Response Management
February 28, 2024

Webinar : Navigating Advertising Laws in India Part II Fireside Chat

service providers; hence it should retain ultimate control over the outsourced activity.

a. PSPs should consider all relevant laws, regulations and conditions of regulatory authorization or licenses when outsourcing functions,
b. Rights of a customer and a participant of payment system against a PSP should not be affected, including grievance redressal,
c. If the PSP has outsourced its customer grievance redressal function, it should provide its customer the option of direct access to its nodal officers for raising or escalating complaints, and
d. In cases wherein the customer has an interface with the service provider, the PSP should clearly indicate to the customer the role of the service provider.

2. Governance: PSPs should have in place a board-approved comprehensive outsourcing policy setting out amongst other things, criteria for selection of outsourcing activities and service providers, parameters for grading the criticality of outsourcing; delegation of authority depending on risks and criticality; and systems to monitor and review the operation of these activities. In addition,

a. The Framework sets out the role of the *board* of the PSP in relation to outsourcing, such as deciding on business activities to be outsourced and approving a framework to evaluate risks and criticality involved in outsourcing.
b. The Framework further confers responsibilities on *senior management* of the PSP in relation to evaluating risks and criticality associated with outsourcing functions, ensuring contingency plans are in place and periodically tested and ensuring an independent review and audit for compliance.
c. All outsourcing arrangements should be maintained in a central record of the PSP, updated and reviewed periodically, and readily accessible to the board and senior management.
d. The PSP should ensure that the service provider has a robust framework for documenting, maintaining and testing business continuity and recovery procedures arising out of outsourced activities, which should be reviewed and tested periodically by the service provider.
e. The PSP should consider availability of alternative service providers, and the prospect of bringing back the outsourced activity in-house in case of an emergency.

Furthermore, the Framework restricts a director or officer or their relatives of a PSP in owning or controlling another service provider, unless it is a group company of the PSP.

3. Outsourcing agreements: The Framework provides certain requirements for the terms and conditions governing the PSP and their service provider. It should be in writing, reviewed by PSP's legal counsel and address risks and strategies for mitigating risks. The agreement should allow the PSP to retain adequate control over the outsourced activity and the right to intervene when necessary for compliance with law.

Key provisions of the outsourcing agreement should include:

a. Defining the activity to be outsourced including service standards,
b. PSP's access to all books, records and information available with the service provider relevant to the outsourced activity,
c. PSP's continuous monitoring and assessment of the service provider,
d. Termination clause and minimum period to execute such provision, if necessary,
e. Service provider's obligation to ensure controls are in place for maintaining confidentiality of customer data,
f. Service provider's liability in case of breach of security and leakage of customer information,
g. Contingency plans to ensure business continuity,
h. Requirement of PSP's prior approval in case of sub-contracting arrangements,
i. PSP's audit rights over the service provider,
j. RBI or RBI authorized persons to access PSP's documents, transaction records and other information stored or processed by the service provider,
k. RBI's right to inspect the service provider and their books of accounts,
l. Service provider's obligations to comply with RBI directions involving activities of the PSP,
m. Service provider's obligation to maintain confidentiality of customer information post expiry or termination of the agreement,
n. Preservation of documents and data by the service provider and protection of PSP's interests post termination of the outsourcing arrangement.

4. Confidentiality and Security: PSP's should ensure that the service provider maintains security and confidentiality of customer information in their custody or possession.

a. Access to the service provider's staff should be limited and on a 'need to know' basis,
b. The service provider should not co-mingle and should be able to isolate and identify the PSP's customer information, documents, records and assets to protect confidentiality,
c. The PSP should regularly review and monitor the security practices and control processed of the service provider,
d. The service provider should report security breaches to the PSP,
e. The PSP should report to the RBI any security breaches and customer confidential information leakages. Liability to customers for such breaches would lie with the PSP.
f. PSPs should ensure that the service provider, whether domestic or offshore, adheres to the RBI's instructions on storage of payment system data.

OUTSOURCING WITHIN GROUP / CONGLOMERATE ENTITIES

with Manisha Kapoor
February 27, 2024

Webinar : Navigating Advertising Laws in India
February 20, 2024

The Framework specifically address PSP's having service arrangements with group entities; for instance, legal and professional services, IT applications, back-office functions, outsourcing payment and settlement services etc. Such arrangements should be based on the PSP's board approved policy and service level arrangements with its group entities.

PSP's should ensure that:

1. The agreements cover demarcation of shared resources like premises, personnel etc.,
2. In case of multiple group entities cross-selling, customers should be informed about the actual entity offering the product or service,
3. The agreements should be in writing and cover details like scope of services, charges and confidentiality of customer data,
4. The arrangement should not cause confusion among customers, as to whose products or services they are availing, by clear physical demarcation of the site of activities of different group entities,
5. The arrangements should not compromise the ability of the PSP to identify and manage risks on a standalone basis,
6. The arrangements should not prevent RBI from obtaining information required for supervision of the PSP or to the group as a whole,
7. The PSP's ability to carry out operations in a sound fashion is not affected if premises or other services like IT or support staff services provided by the group entity are interrupted,
8. Risk management practices adopted by PSP's for outsourcing to group entities should be the same as prescribed in the Framework for a non-related party.

OUTSOURCING TO OVERSEAS ENTITIES

The PSP should monitor Government policies, 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. Contingency and exit strategies should be in place.

In outsourcing services relating to Indian operations to offshore entities, the PSP should ensure that:

1. In principle, arrangements should be with parties in jurisdictions that generally uphold confidentiality clauses and agreements,
2. The governing law of the agreement is clearly specified,
3. The activities outsourced should be conducted in a manner to not hinder efforts to supervise or reconstruct the India activities of the PSP,
4. The offshore regulator should not obstruct to the arrangement nor object to RBI's visits for audit, scrutiny, examination, inspection, assessment or visits from PSP's internal and external auditors,
5. The offshore regulator does not have access to the data relating to the PSP's India operations, and
6. The jurisdiction of courts in the offshore jurisdiction does not extend to the PSP's operations in India merely because data is processed in the offshore location.

PARTICIPANTS IN THE PAYMENTS ECOSYSTEM

The PSP should also engage with all participants in a payment transaction to *encourage* them to implement the Framework. Specifically, in respect of payment systems operated by PSPs involving other participants such as token requestors in tokenization solutions, third-party application providers in UPI systems etc. who may not be directly regulated or supervised by RBI; but it is prudent for such participants to put in place systems to manage risks arising out of activities outsourced by them.

The above provisions from the Framework do not appear to relate *per se* to outsourcing activities, though appear to suggest that non-licensed entities in the payment's ecosystem are encouraged to adopt appropriate security and risk mitigation measures.

ANALYSIS

Firstly, payment intermediaries were historically not directly regulated by the RBI but instead since 2009, were indirectly via AD banks with whom they needed to have nodal accounts for settlement of transactions between merchants and consumers. In a paradigm shift since March 2020, payment intermediaries that handle the funds, in receiving, pooling and transferring funds from customers to merchants were directly regulated and put under a licensing regime by the RBI. This was the first step to regulating payment aggregators, a type of a PSP. However, certain other PSPs were and continue to be regulated under the PSS Act and RBI regulations, for instance, e-wallet and gift instrument issuers. In fact, PSPs are being drawn a wider net of regulation in recent years, given the important role that they play in payment transactions, for instance imposition of data localization norms. Having said that, *outsourcing functions of PSPs* were not previously regulated, unlike in the case of banking and non-banking financial companies (NBFCs) wherein specific RBI directives were issued on the subject. Hence, this is a first of its kind regulation for outsourcing functions of PSPs.

Secondly, the Framework doesn't substantially differ from the previous RBI directives on outsourcing applicable to banks and NBFCs which also contained provisions along the same lines such as control and supervision, risk assessments and policies, confidentiality and security, outsourcing agreements, outsourcing restrictions, grievance redressal and outsourcing within group entities / conglomerates, and to offshore service providers. Hence, whilst the Framework is a first for PSPs, it appears to only follow precedent that the RBI has set in regulating outsourcing functions by regulated entities, though more sophisticated. This entails that PSPs would follow the route taken by banks and NBFCs in terms of governance and contractual compliances when outsourcing functions to service providers.

Thirdly, the Framework restricts outsourcing of 'core management functions', which includes some of the obvious functions meant to be carried out directly by the PSP such as management of payment system operations,

transactions and risk management, audits, compliance and decision-making functions. However, managing customer data and IT and InfoSec management is also considered a 'core management function' that cannot be outsourced. Further, customer data is defined to include payments-related data / information. Basis this and considering the recent data storage restrictions, it will be interesting to see how the industry views "management" especially in the context where data storage / processing functions are outsourced but the PSP continues to retain overall control / rights over the data. In such situations it would need to be evaluated whether the same would be viewed as outsourcing of a core management function.

Similarly, it is common for banks, NBFCs and even PSPs to engage service providers for IT and InfoSec services and to provide systems and solutions for the former's business operations. Such arrangements would also need to be evaluated to determine whether it constitutes outsourcing of 'management' functions.

Also, the Framework identifies 'core management functions' in a non-exhaustive manner by using the term "including". Thus, unless clarified by the RBI, it would always be subjective and open to interpretation on what other functions would be deemed to be 'core management functions' which should not be outsourced by PSPs.

Finally, from a cross-border perspective, PSPs would need to evaluate existing and future arrangements keeping in mind additional requirements. Requirements for the PSP to ensure that the offshore regulator does not object to RBI/PSP's visits and audits and does not access the data to the PSP's India operations and offshore Courts' jurisdiction does not extend to PSP's operations in India; go beyond the offshore outsourcing provisions applicable to banks and NBFCs. PSPs would need to implement extra steps and assessments which may include understanding and taking legal opinions on applicable foreign laws prior to entering into such offshore outsourcing arrangements, as well as tailor the outsourcing agreements to address the cross-border requirements.

CONCLUSION

From a user perspective, this Framework is a welcome step where non-bank PSPs would be subject to outsourcing compliances which would largely benefit consumer interest. This is also in line with the existing outsourcing regulations as applicable to banking and non-banking financial companies.

However, given the advancements in technology and security solutions along with business prowess of new fintech players including PSPs, outsourcing certain activities relating to managing customer data, IT services and InfoSec functions should be permitted subject to relevant compliances under the Framework.

Consumer interests could still be protected as PSPs would need to comply with the Framework including implementation of risk evaluation policies, security standards, audits, controls and stringent contractual arrangements with third party service providers. Thus, categorizing the said activities as 'core management functions' which cannot be outsourced may impact the growth and innovation of the industry.

– Aaron Kamath & Huzefa Tavawalla

You can direct your queries or comments to the authors

[1] Section 2(i) of the PSS Act.

[2] Though is not applicable to activities not relating to payment / settlement services, such as internal administration, housekeeping or similar activities.