भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2021-22/76
CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 August 3, 2021

The Chairman / Managing Director / Chief Executive Officer
All Non-Bank Payment System Operators

Madam / Dear Sir,

Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators

The Payment System Operators (PSOs), by virtue of services they provide and the construct of models on which they operate, largely outsource their payment and settlement-related activities to various other entities.

2. In order to enable effective management of attendant risks in outsourcing of such activities, it was announced in the Statement on Developmental and Regulatory Policies released with the bi-monthly Monetary Policy Statement 2020-21 on February 05, 2021, that a framework for outsourcing of payment and settlement-related activities by PSOs, will be issued by the Reserve Bank of India. Accordingly, a framework for the same is provided in the Annex. The PSOs shall ensure that all their outsourcing arrangements, including the existing ones, are in compliance with this framework by March 31, 2022.

3. This framework is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

Yours faithfully,

(P Vasudevan)
Chief General Manager

भुगतान और निपटान प्रणाली विभाग, केंद्रीय कार्यालय, 14वी मंजिल, केंद्रीय कार्यालय भवन,शहीद भगत सिंह मार्ग, फोर्ट, मुम्बई - 400001
फोन Tel: (91-22) 2264 4995; फैक्स Fax: (91-22) 22691557; ई-मेल e-mail : cgmdpssco@rbi.org.in
Department of Payment and Settlement Systems, Central Office, 14th Floor, Central Office Building, Shahid Bhagat Singh Road, Fort, Mumbai - 400001

Annex

(RBI circular CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 3, 2021)

Framework for Outsourcing of Payment and Settlement-related activities by PSOs[1]

1. **Introduction**

1.1. This framework is applicable to non-bank PSOs insofar as it relates to their payment and / or settlement-related activities.

1.2. It seeks to put in place minimum standards to manage risks in outsourcing of payment and / or settlement-related activities (including other incidental activities like on-boarding customers[2], IT based services, etc.).

1.3. The framework is not applicable to activities other than those related to payment and / or settlement services, such as internal administration, housekeeping or similar functions.

1.4. For the purpose of this framework, 'outsourcing' is defined as use of a third party (i.e. service provider) to perform activities on a continuing basis that would normally be undertaken by the PSO itself, now or in the future. 'Continuing basis' would include agreements for a limited period.

1.5. The term 'service provider' includes, but is not limited to, vendors, payment gateways, agents, consultants and / or their representatives that are engaged in the activity of payment and / or settlement systems. It also includes sub-contractors (i.e., secondary service providers) to whom the primary service providers may further outsource whole or part of some activity related to payment and settlement system activities outsourced by the PSO.

1.6. This framework is applicable to a service provider, whether located in India or elsewhere.

1.7. The service provider, unless it is a group company of the PSO, shall not be owned or controlled by any director or officer of the PSO or their relatives; the terms – control, director, officer and relative – have the same meaning as assigned to them under the Companies Act, 2013.

1.8. Outsourcing process is associated with several risks; following is an illustrative list of such risks:

---

[1] As per the Payment and Settlement Systems Act, 2007, a "system provider" means a person who operates an authorised payment system. The terms *'Provider'* and *'Operator'* have been used interchangeably in this framework.

[2] The word "customer" wherever used in this framework includes the end-user, i.e., general public, who uses the payment system product(s). Further, customer data / information includes payments-related data / information also.

a) Compliance Risk – Where privacy, customer / consumer and prudential laws are not adequately complied with by the service provider;
b) Concentration and Systemic Risk – Where the overall industry has considerable exposure to one service provider and hence, individual PSO may lack control over the service provider;
c) Contractual Risk – Where the PSO may not have the ability to enforce the contract;
d) Country Risk – When political, social or legal climate creates added risk;
e) Cyber Security risk – Where breach in IT systems may lead to potential loss of data, information, reputation, money, etc.;
f) Exit Strategy Risk – When over-reliant on one firm, the PSO loses related skills internally, and it becomes difficult to bring the activity back in-house; and where the PSO has entered into contracts that makes speedy exit prohibitively expensive;
g) Legal Risk – Where the PSO is subjected to fines, penalties, or punitive damages resulting from supervisory actions, as well as to private settlements due to acts of omission and commission by the service provider;
h) Operational Risk – Arising due to technology failure, fraud, error, inadequate financial capacity to fulfil obligations and / or to provide remedies;
i) Reputation Risk – Where the service provided is poor and customer interaction is inconsistent with the overall standard expected from the PSO; and
j) Strategic Risk – Where the service provider conducts business on its own behalf, inconsistent with the overall strategic goals of the PSO.

1.9. It is essential that the PSO, which is outsourcing its activities, ensures the following:
a) Exercises due diligence, puts in place sound and responsive risk management practices for effective oversight, and manages the risks arising from such outsourcing of activities.
b) Outsourcing arrangements do not impede its effective supervision by RBI.

1.10. Outsourcing of activities by the PSOs shall not require prior approval from RBI.

2. Activities that shall not be outsourced

2.1. The PSOs shall not outsource core management functions[3], including risk management and internal audit; compliance and decision-making functions such as determining compliance with KYC norms. However, while internal audit function itself

[3] Core management functions should include, but not be confined to, management of payment system operations (netting, settlement, etc.); transaction management (reconciliation, reporting and item processing); according sanction to merchants for acquiring; managing customer data; risk management; information technology & information security management; etc.

is a management process, the auditors for this purpose can be appointed by the PSO from its own employees or from the outside on contract.

3. Criticality of outsourcing

3.1. The PSO shall carefully evaluate the need for outsourcing its critical processes and activities, as also selection of service provider(s) based on comprehensive risk assessment. The critical processes are those, which if disrupted, shall have the potential to significantly impact the business operations, reputation, profitability and / or customer service.

4. PSO's role and regulatory and supervisory requirements

4.1. Outsourcing of any activity by the PSO shall not reduce its obligations, and those of its board and senior management, who are ultimately responsible for the outsourced activity. The PSO shall, therefore, be liable for the actions of its service providers and shall retain ultimate control over the outsourced activity.

4.2. The PSO, while exercising due diligence in respect of outsourcing, shall consider all relevant laws, regulations, guidelines and conditions of authorisation / approval, licensing or registration.

4.3. Outsourcing arrangements shall not affect the rights of a customer of a payment system against the PSO, as well as those of a payment system participant against the PSO, including her / his ability to avail grievance redressal as applicable under the relevant laws. Responsibility of addressing the grievances of its customers shall rest with the PSO, including in respect of the services provided by the outsourced agency (i.e., service provider).

4.4. A PSO, which has outsourced its customer grievance redressal function, must also provide its customers the option of direct access to its 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 shall be displayed prominently on its website, mobile applications, advertisements, etc., and adequate awareness shall also be created about the availability of this recourse.

4.5. If the customer is required to have an interface with the service provider to avail products of the PSO, then the PSO shall state the same through the product literature / brochure, etc., and also indicate therein the role of such service provider.

4.6. A PSO must ensure that outsourcing does not impede or interfere with the ability of the PSO to effectively oversee and manage its activities; nor does it prevent RBI from carrying out its supervisory functions and objectives.

5. Outsourcing policy

5.1. To outsource any of its payment and settlement-related activities, the PSO shall have a board-approved comprehensive outsourcing policy, which incorporates, inter-alia, criteria for selection of such 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.

6. Role of the board and responsibilities of the senior management

6.1. Role of the board

The board of the PSO, or a committee of the board to which powers have been delegated, shall be responsible, inter-alia, for the following:

a) approving a framework to evaluate the risks and criticality of all existing and prospective outsourcing;
b) approving policies that apply to outsourcing arrangements;
c) mapping appropriate approval authorities for outsourcing depending on risks and criticality;
d) setting up suitable administrative mechanism of senior management for the purpose of this framework;
e) undertaking periodic review of outsourcing policy, strategies and arrangements for their continued relevance, safety and soundness;
f) deciding on business activities to be outsourced and approving such arrangements; and
g) complying with regulatory instructions.

6.2. Responsibilities of the senior management

The senior management shall be responsible for:

a) evaluating the risks and criticality of all existing and prospective outsourcing, based on the framework approved by the board;
b) developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing activity;
c) reviewing periodically the effectiveness of policies and procedures, and for identifying new outsourcing risks as they arise;
d) communicating, in a timely manner, to the board any information related to outsourcing risks;
e) ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested periodically; and
f) ensuring an independent review and audit for compliance with the set policies.

6.3. A central record of all outsourcing arrangements shall be maintained and it shall be readily accessible for review by the board and senior management of the PSO. The record shall be updated promptly, and half yearly reviews shall be placed before the board or its senior management.

7. Evaluating capability of the service provider

7.1. While considering / renewing an outsourcing arrangement, the PSO shall include issues related to undue concentration of such arrangements with a service provider.

8. Outsourcing agreement

8.1. The terms and conditions governing the contract between the PSO and the service provider shall be carefully defined in written agreements and vetted by PSO's legal counsel for their legal effect and enforceability. Every such agreement shall address the risks and the strategies for mitigating them. The agreement shall be sufficiently flexible to allow the PSO to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement shall also bring out the nature of legal relationship between the parties, i.e. whether agent, principal or otherwise. Some of the key provisions of the agreement should incorporate the following:

a) defining activity to be outsourced, including appropriate service and performance standards;
b) having access by the PSO to all books, records and information relevant to the outsourced activity, available with the service provider;
c) providing for continuous monitoring and assessment by the PSO of the service provider, so that any necessary corrective measure can be taken immediately;
d) including termination clause and minimum period to execute such provision, if deemed necessary;
e) ensuring controls are in place for maintaining confidentiality of customer data and incorporating service provider's liability in case of breach of security and leakage of such information related to customers;
f) incorporating contingency plan(s) to ensure business continuity;
g) requiring prior approval / consent of the PSO for use of sub-contractors by the service provider for all or part of an outsourced activity;
h) retaining PSO's right to conduct audit of the service provider, whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the PSO;

i) adding clauses to allow RBI or person(s) authorised by it to access the PSO's documents, record of transactions and other necessary information given to, stored or processed by the service provider, within a reasonable time;

j) keeping clauses to recognise the right of RBI to cause an inspection to be made of a service provider of a PSO and the books of accounts, by one or more of its officers or employees or other persons;

k) requiring clauses relating to a clear obligation on any service provider to comply with directions given by RBI insofar as they involve activities of the PSO;

l) maintaining confidentiality of customer's information even after the agreement expires or gets terminated; and

m) preserving documents and data by the service provider in accordance with legal / regulatory obligations of the PSO, and the PSO's interests in this regard shall be protected even after termination of the services.

9. **Confidentiality and security**

9.1. Public confidence and customer trust in the PSO is a prerequisite for its stability and reputation. PSO shall ensure the security and confidentiality of customer information in the custody or possession of the service provider.

9.2. Access to customer information by staff of the service provider shall be on 'need to know' basis, i.e., limited to areas where the information is required to perform the outsourced function.

9.3. The service provider shall be able to isolate and clearly identify the PSO's customer information, documents, records and assets to protect their confidentiality. Where the service provider acts as an outsourcing agent for multiple PSOs, there should be strong safeguards (including encryption of customer data) to avoid co-mingling of information, documents, records and assets of different PSOs.

9.4. The PSO shall regularly review and monitor the security practices and control processes of the service provider and require the service provider to disclose security breaches.

9.5. The PSO shall immediately notify RBI about any breach of security and leakage of confidential information related to customers. In such eventualities, the PSO would be liable to its customers for any damage.

9.6. The PSO shall ensure that the extant instructions related to storage of payment system data shall be strictly adhered to by service provider, domestic or off-shore.

10. **Responsibilities of Direct Sales Agents (DSAs) / Direct Marketing Agents (DMAs)**

10.1. The PSOs shall ensure that the DSAs / DMAs are properly trained to handle their responsibilities with care and sensitivity, particularly for aspects such as soliciting

customers, hours of calling, privacy of customer information, conveying the correct terms and conditions of the products on offer, etc.

10.2. The PSOs shall put in place a board-approved code of conduct for DSAs / DMAs and obtain their undertaking to abide by the same.

11. Business continuity and management of disaster recovery plan

11.1. Service provider shall develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures arising out of any outsourced activity. The PSO shall ensure that the service provider periodically tests the business continuity and recovery plans, and shall also consider conducting occasional joint exercises for testing of business continuity and recovery procedures with its service provider.

11.2. To mitigate risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, the PSO shall retain adequate control over its outsourcing and shall have the right to intervene with appropriate measures to continue its business operations and its services to the customers in such cases without incurring prohibitive expenses or any break in its operations and services to the customers.

11.3. As part of contingency plan, the PSO shall consider the availability of alternative service provider(s), as well as the possibility of bringing the outsourced activity back in-house in an emergency and assess the cost, time and resources that would be involved.

11.4. The PSO's information, documents and records, and other assets shall be isolable by the service provider. This is to ensure that in appropriate situations, all documents, record of transactions and information given to the service provider, and assets of the PSO, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

12. Monitoring and control of outsourced activities

12.1. The PSO shall put in place a management structure to monitor and control its outsourcing activities. It shall ensure that outsourcing agreement with the service provider contains provisions to address monitoring and control by it of the outsourced activities.

12.2. Regular audit by either the internal or external auditors of the PSO shall be conducted to assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangements and the PSO's compliance with its risk management framework.

12.3. The PSO shall, at least on an annual basis, review the financial and operational conditions of the service provider to assess its ability to fulfil its outsourcing obligations.

Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

12.4. In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers, the same shall be given due publicity by the PSO informing the customers so as to ensure that they stop dealing with the concerned service provider.

12.5. Certain cases like outsourcing of cash management, may involve reconciliation of transactions between the PSO, the service provider and its sub-contractors, if any. In such cases, PSO shall ensure that this reconciliation process is carried out in a timely manner.

12.6. A robust system of internal audit of all outsourced activities shall be put in place and monitored by the board of the PSO.

13. **Outsourcing within a group / conglomerate**

13.1. The PSO could have back office and service arrangements / agreements with group entities; for instance, sharing of premises, legal and other professional services, hardware and software applications, centralised back office functions, outsourcing certain payment and settlement services to other group entities, etc. Such arrangements with group entities shall be based on the PSO's board-approved policy and service level arrangements / agreements with its group entities. The agreements shall cover demarcation of shared resources like premises, personnel, etc. Wherever there are multiple group entities involved or any cross-selling is observed, the customers shall be informed about the actual company / entity offering the product / service.

13.2. The PSO shall ensure that such arrangements:

a) are appropriately documented in written agreements with details like scope of services, charges for services and maintaining confidentiality of customer's data;

b) do not cause any confusion among customers as to whose products / services they are availing, by clear physical demarcation of the site of activities of different group entities;

c) do not compromise ability of the PSO to identify and manage risks on a standalone basis; and

d) do not prevent RBI from being able to obtain information required for supervision of the PSO or pertaining to the group as a whole.

13.3. The PSO shall ensure that its ability to carry out operations in a sound fashion is not affected if premises or other services (such as IT systems and support staff) provided by the group entities become unavailable.

13.4. If sharing of premises is done with the group entities for cross-selling, the PSO shall take measures to ensure that the entity's identification is distinctly visible and clear to the customers. Any communication by group entities (marketing brochure, verbal communication by staff / agent, etc.) in the PSO's premises shall mention nature of arrangement of the entities with the PSO, so that customers are clear about the seller of the product.

13.5. The PSO's advertisement or any agreement shall not give any overt or tacit impression that it is in any way responsible for the obligations of its group entities.

13.6. The risk management practices to be adopted by the PSO while outsourcing to a related party (i.e. party within the group / conglomerate) shall be identical to those specified above in this framework for a non-related party.

14. **Additional requirements for off-shore outsourcing**

14.1. The engagement of a service provider in a foreign country exposes the PSO to country risk. To manage such country risk, the PSO shall 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. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

14.2. The activities outsourced outside India shall be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of the PSO in a timely manner.

14.3. As regards off-shore outsourcing of its services relating to Indian operations, the PSO shall ensure the following:

a) The off-shore regulator regulating the off-shore service provider shall neither obstruct the arrangement nor object to RBI's visit(s) for audit / scrutiny / examination / inspection / assessment or visit(s) by PSO's internal and external auditors;

b) The regulatory authority of the off-shore location does not have access to the data relating to Indian operations of the PSO simply on the ground that the processing is being undertaken there (not applicable if off-shore processing is done in the home country of the PSO); and

c) The jurisdiction of the courts in the off-shore location where data is processed, does not extend to the operations of the PSO in India on the strength of the fact that the

data is being processed there even though the actual transactions are undertaken in India.

15. **Members / Participants of payment systems operated by the PSOs**

15.1. In some payment systems operated by the PSOs, there could be other members / participants also. Some of these entities such as token requestors in tokenisation services rendered by card networks, third party application providers in Unified Payments Interface (UPI), etc., may not be directly regulated or supervised by RBI. Many of these entities may provide payment services directly to customers as well. It is prudent for such entities to put in place a system to manage risks arising out of activities outsourced by them.

15.2. As a best practice, the PSOs may engage with all participants in a payment transaction chain to encourage them to implement this framework in letter and spirit.

****