NPCI/2024-25/RMD/006 01st January 2025

To,

All Member/Sub Member and PSP banks

Sir/ Madam,

Subject: Directions to member banks, NPCI partners on Managing Third Party Risks.

Third Party risks are potential threats to the organizations and to the ecosystem due to their reliance on external entities- such as vendors, Suppliers, Contractors etc., which provide goods, services or support. This risk arises from the possibility that these third parties may introduce vulnerability such as security breaches, operational and process failures, regulatory non-compliances, or reputational risk to the organization and to the ecosystem.

Managing third party risk involves assessing, monitoring and mitigating these risks to ensure the organization's/ ecosystem security, compliance and continuity of operations.

In this regard NPCI would like its partners (Member banks, Sub member, PSP's and other entities such as ASP's, TSP's etc.) to follow the directions given below on Third-party Risk Management (TPRM):

- Establish and follow robust third-party risk management practices to supervise its vendors supporting NPCI products.
- Perform an appropriate level of due diligence of its service providers/Third Parties. A risk-based approach should be followed for due diligence, considering various factors like qualitative, quantitative, financial, operational, legal, reputational and geographical.
- Ensure that the rights and obligations towards each of their service providers are clearly defined and set out in a legally binding written agreement.
- Establish a management structure to monitor and control the outsourced activities related to NPCI and its products, including but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.
- Conduct periodic audits of third-party service providers supporting NPCI products and the audit results shall be made available to NPCI. Establish a Board-approved policy and appropriate service level agreements with its group entities in case partners have outsourced any activities related to NPCI products within its business group/conglomerate.

- Ensure any engagement with service provider based in a different jurisdiction shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk.
- Ensure the rights of Partner, NPCI and the Regulator to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction and the arrangement shall comply with all statutory requirements as well as regulations issued by the Regulator from time to time.
- Establish a clear exit strategy regarding outsourced services, while ensuring business continuity during and after exit. Partner shall identify alternative arrangements, which may include performing the activity by a different service provider or Partner itself.
- Ensure that the agreement with their third parties shall have necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable.

Yours sincerely,

SD/-

Viswanath Krishnamurthy

Chief Risk Officer