

On-soil storage of Payments Data

Point of View

July 2018



E **Foreword**

Dear Readers,

It is my pleasure to bring to you the latest edition of our Payments newsletter, where we explore the implications of the RBI circular mandating Payments system data to be stored only in India. As we move towards more advanced technologies in the way payments are accepted and paid, it becomes imperative to focus towards improved accessibility and security measures.

In addition to our views, based on our expertise across the Fintech and payments landscape along with insights from our work with clients, we have captured key challenges and ways in which organizations can adapt to the change to become compliant to the data storage norms as per RBI's guidance.

I hope you will find this to be an insightful read.

For details or feedback, please write to

vivek.belgavi@in.pwc.com or mihir.gandhi@in.pwc.com



Vivek Belgavi

Partner

*Financial Services Technology
Consulting Leader, PwC*



I *In this issue*

Foreword

Introduction

Impact and Next Steps

Payments Technology Updates

I Introduction

With the growth of digital payments in the country, there has been a significant increase in the data generated through payment transactions. Increasingly, there are new players and participants in the payments ecosystem offering unique use-cases and novel payment solutions to customers in India. In light of such ubiquitous data there has been an imminent need for enhanced supervision by authorities and for safeguarding **access** and **storage** of data, especially, given that many global players have their databases and processing systems in locations across the world. Consequently, in a bid to have unfettered supervisory access to data stored with system providers, the Reserve Bank of India issued a circular on 6 April'18 on "Storage of Payment System data". This circular mandated the storage of entire data related to payment systems operated by system providers, in a system *only* in India.

The RBI directive has far reaching implications as the mandate not only impacts authorized payment systems, but also several other players in the payments value chain such as service providers, intermediaries, third party vendors.

One of the key points raised by impacted players is that the mandate is for storage of entire payments related data **only** in India. This essentially prohibits players from sharing any data to their centralized servers for fraud monitoring, or for serving as back-up repository. The circular also states that the requisite data should include end-to-end transaction details/ information collected/ carried/ processed as part of the message/ payment instruction. This widens the horizon of the data in consideration and creates ambiguity on whether such data includes only transaction information or data related to customer identification as well.

The Circular

Background

- In light of recent personal data privacy breach incidents
- China, Japan, Malaysia have similar regulatory requirement for data storage

Objectives

- Security, confidentiality and access to payments and customer data

Quick Facts

- Compliance by 15th Oct, 2018
- Audit through CERT-in certified auditor by 31 Dec, 2018
 - End-to-end transaction details
- For the foreign leg, data can **also** be stored outside, if required

RBI has also mandated all payments system providers to submit a System Audit Report on completion of the exercise and is subsequently seeking fortnightly updates about progress on the implementation of the mandate. However, it is unclear if a separate bench at the Apex body will monitor these.

While the initial circular was brief and multiple interpretations were doing rounds, it is expected that the RBI will soon publish a detailed Frequently Asked Questions (FAQ) document for further clarifications.

Impact and Next Steps

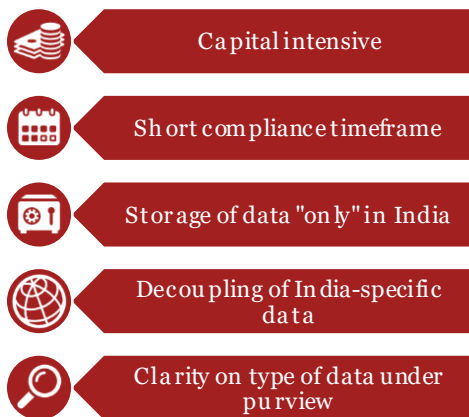
ownership and control, deploying a new data center is expensive and time consuming as it

Stakeholders that may be impacted

Most Indian Banks and PPI players are already in compliance with requirements stated in this circular, however players such as foreign banks international card networks, new age FinTechs using on-cloud services that are hosted internationally, payment intermediaries involved in processing and authentication need to take immediate action to comply.

While the mandate will benefit Indian hosted data center providers, it may also act as an entry barrier for future players looking to enter the Indian payments ecosystem.

Challenges



Way Forward

Considering the objectives with which the RBI has setup this mandate and is seeking regular updates from impacted stakeholders, it would be prudent for banks and payments service providers to devise their strategy and take immediate action to ensure compliance to the circular. Listed below are options that may be considered-

I. Setting-up a own data center:

This would entail setting up both IT components viz. servers, storage, networking devices and Non-IT components viz. cabling, cooling, batteries, power backup, security. While one's own data center provides complete

entails numerous activities such as finding the right location, hiring IT and non-IT vendors, deploying resources to build and maintain it, deploying offsite DR system, certifications such as PCI DSS/ PA-DSS, security audits as applicable. Setting up such a data center for a large player can take anywhere between 12- 18 months and end up becoming one of the large projects a company undertakes.

Data Center in a Box which is a portable, self-contained computing facility that integrates all elements of a traditional DC can be considered for quick deployment

II. Hosting in a Multi-Tenant setup:

Hosting in a co-located managed data center can enable flexibility, scalability, ensure costs get allocated over a longer time while ensuring high availability and efficiency. As long as there is strategic long term benefit and an appetite for such investments, buying out an existing hosted data center business may also be considered for achieving quick turnaround and compliance.

III. Hosting On-Cloud:

Private cloud hosting with ring-fenced resources can be considered as a quick, secure and flexible solution. This is subject to the underlying network of physical servers being hosted locally (as the circular has 'only' clause). This may also prove to be cost effective for players having spikes in demand utilization.

There are alternatives available to building and expanding one's data center, areas like business needs, capital costs, growth expectations, data security and staffing requirements need to be explored. A phase wise migration for primary and then DR to on-soil systems may be an alternative that results in higher compliance in adhering to the timelines.

(With inputs from Mihir Gandhi, Neha Jaeel, Jaya Gupta, Neema Kar)

*P*ayments Technology Updates

RBI Mandates Domestic Storage of Payments

BankInfoSecurity

The Reserve Bank of India is requiring that payment system ... The RBI mandate for domestic storage of all data must be met by October 15

[\(Read more\)](#)

RBI: Store payment data only in India

ET
Payment data All payment system operators will have to ensure that data related to payments is stored only in India.

[\(Read more\)](#)

Views of Industry Experts on Reserve Bank of India Notification

Mondaq

India is aiming towards being a paperless economy. For the past one year, digitization has taken India by storm.

[\(Read more\)](#)

RBI mandates data localization for payment systems

Lexology

RBI's move on data localization to payment systems comes as a probable aftermath of the recent data breach that has allegedly impacted elections in US and India.

[\(Read more\)](#)

RBI issues notification on data storage by payment companies

Finextra

The operators have been asked to comply with the instructions within six months, the central bank said in a notification. RBI noted that "not all system providers" store the payments data in India.

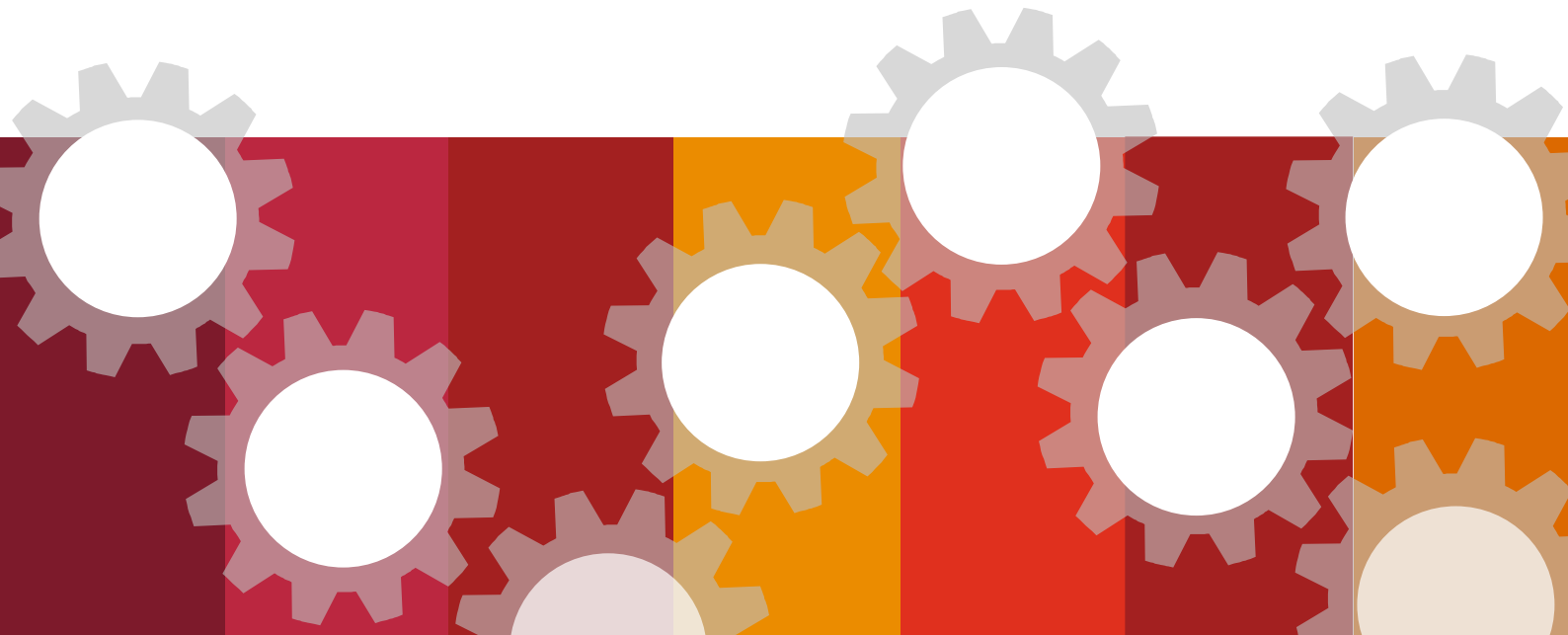
[\(Read more\)](#)

Norm on Storage of Payment System Data by RBI

SISA

Considering the current trend in data storage technology, data is usually kept in multiple locations in order to have back up for data centers.

[\(Read more\)](#)



P ***Please contact***

For more information, please contact:

Vivek Belgavi

Partner – Financial Services Technology

Tel: +91 9820280199

Email: vivek.belgavi@pwc.com

Mihir Gandhi

Partner – Payments Transformation

Tel: +91 9930944573

Email: mihir.gandhi@pwc.com