September, 2021

India Update: RBI Tokenisation Framework

On September 7, 2021, the Reserve Bank of India ("**RBI**") released circular CO.DPSS.POLC.No.S-516/02-14-003/2021-22 ("**CoFT Circular**") updating the framework for card tokenisation in India. The updated framework extends this technology to Card-on File Tokenisation ("**CoFT**") and now allows card issuers to offer tokenisation services.

Previous Framework

On January 8, 2019, the RBI permitted authorised card payment networks ("**Card Networks**") to offer card tokenisation services to third-party app providers ("**Token Requestors**"). The RBI allowed Card Networks to offer tokenisation for all use cases, including near field communication (NFC) / magnetic secure transmission (MST) based contactless transactions, in-app payments, and QR code-based payments. However, Card Networks were only allowed to enable tokenisation through trusted devices – originally, mobile phones and tablets and more recently, IoT devices and wearables. This means that any 'token' issued by a Card Network in place of actual card details must be linked to a specific device.

Stakeholders in the payments industry have repeatedly urged the RBI to create a more permissive tokenisation framework that looks beyond device-based tokenisation. Merchants, payment intermediaries and industry bodies have requested the regulator to allow cloud-based tokenisation, a mechanism whereby customers and merchants can create and retrieve tokens regardless of the device used by the consumer to initiate payment transactions. These demands have become particularly clamorous since the RBI's recent directive[1] effectively banning payment aggregators and e-commerce merchants from storing customer card details on their systems.

Updated Framework

The RBI appears to have finally taken heed of the concerns voiced by the industry and has now permitted CoFT. Some of the notable features of the CoFT Circular and our inputs and comments have been summarised below:

1. **Cloud-based Tokenisation**: While the RBI's existing tokenisation framework relies on trusted-devices, i.e., mobile phones, tablets etc., the new framework allows for cloud-based tokenisation, whereby tokens are not linked to a particular device. This marks a significant and positive departure from the existing

[1] See Paragraph 6.2 and 6.3 of the Annex of RBI circular CO.DPSS.POLC.No.S33/02-14-008/2020-2021 dated March 31, 2021.

regulatory framework. Several stakeholders, particularly e-commerce merchants, have complained since 2019 that device-based tokenisation would be unfeasible to practically implement and is an inadequate substitute for actual card credentials.

2. **Issuers permitted to Tokenize**: The RBI's CoFT Circular permits issuing banks to provide tokenisation services (in addition to Card Networks) and to act as token service providers ("**TSPs**"). Such TSPs are permitted to offer tokenisation services only for cards issued by or affiliated with them and are responsible for ensuring compliance with the framework.
3. While notable, it remains to be seen how issuing banks would practically enable CoFT on a large scale. In practice, merchants may prefer utilizing the tokenisation services of Card Networks, so as to avoid separately engaging/contracting with multiple issuing banks.
4. **Streamlined AFA**: The requirement for additional factor of authentication (AFA) continues to apply to tokenisation under the updated framework. However, the RBI has clarified that AFA validation may be combined and undertaken simultaneously where a card payment transaction and a registration for CoFT are performed at the same time. This would come as a relief for e-commerce merchants who had complained of the friction caused by the multiple AFA validations mandated under the RBI's previous framework.
5. **Restrictions on Data Storage**: The RBI has taken this opportunity to reiterate its stance on card data storage. As per the CoFT Circular, no entity in the card transaction / payment chain, other than TSPs, are permitted to store any card data with effect from January 01, 2022. Most notably, the RBI has directed all such entities to delete data previous stored from their systems.
6. This requirement to purge or delete card data is important and should be noted by any e-commerce company that proposes to house such data in card vaults or similar systems hosted by affiliate and third party entities.
7. **Clarity on "Limited Data"**: As an exception to the above restrictions, the RBI has clarified that non-TSP entities may continue to store (a) the last four digits of the actual card number; and (b) the card issuer's name ("**Limited Data**") for transaction tracking and/or reconciliation purposes.
8. While merchants and fintech companies had craved for further clarity on the scope of Limited Data (since the RBI's clarifications in the PA/PG Guidelines), the RBI's definition appears much narrower than what most stakeholders may have hoped for. This statement may take companies back to the drawing board and may need them to re-evaluate their mechanisms for payment tracking and transaction fulfilment.

For further details, please contact km@jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi

