RBI’s Card Tokenisation Notification: Guidelines and Legal Implications
written by Abhilasha SG | July 2, 2022

RBI Card Tokenization - Guidelines

The payments industry is developing to accommodate new payment form factors, necessitating increased security measures to prevent account fraud and counterfeiting. Card-present, card-not-present, and hybrid transactions all require excellent security to reduce the risk of unauthorized access to cardholder account data and to avoid cross-channel fraud. Tokenization provides a lot of potential for meeting this necessity.

What Is Tokenisation?

According to the Reserve Bank of India [RBI], tokenisation refers to “the replacement of actual card details with an alternate code called the “token”, which shall be unique for a combination of card, token requestor (i.e., the entity which accepts a request from the customer for tokenization of a card, and passes it on to the card network to issue a corresponding token) and device (referred hereafter as “identified device”).” [1]

RBI’s Notification

On January 8th 2019, the RBI published a permission circular to initiate the card tokenization process to increase the security of India’s payment ecosystem [2]. With the help of card networks, banks might potentially offer tokenisation services to owners of debit, credit, and prepaid cards. This permission is valid for all token storage and use channels.

In a circular dated December 23rd 2021, the RBI extended the deadline for this obligatory tokenization procedure till June 30th 2022 [3]. This was done in an extension to the previous March 2020 deadline. As a result, it is critical to stress that companies other than card issuers and networks must erase previously saved card data. The card issuer's name and the final four digits of the actual card number are the only exceptions to this rule.

The guidelines were laid down on the following criteria:

- Authorization and Capital Requirements
- Governance and Anti-Money Laundering Objectives
- Merchant On-boarding
- Settlement and Escrow Account Management
- Security and Risk Management Framework

Authorization And Capital Requirements

The “Guidelines on Regulation of Payment Aggregators and Payment Gateways” make it mandatory for Payment Aggregators [PAs] & Payment Gateways

[PGs] to get authorized via the RBI before June 30th 2022 based on their roles in handling funds as intermediaries. Their nature and role shall be clarified in their Memorandum of Association [MOA].
Furthermore, the PAs shall have a net worth of ₹15 crores as of March 31st 2021 and a net worth of ₹25 crores on or before March 31st 2023. A net worth of ₹25 crores shall be maintained at all times thereafter. To showcase the net worth, the entities must submit a certificate from their chartered accountant to show proof of compliance with applicable net-worth requirements while applying for authorization.
In cases of Foreign Direct Investments [FDIs], the Consolidated Foreign Direct Investment Policy of India and the appropriate foreign exchange management rules on this issue shall be referred to i.e., the Foreign Exchange Management Act & the Foreign Exchange Regulation Act.
Card-on-File Tokenization [CoFT] services are now available in the tokenization system. The token must be exclusive to the card, token requestor, and merchant when used for this purpose. Card issuers can now act as Token Service Providers [TSPs] in providing card tokenization services. TSPs can only provide this service for cards issued by or linked to them. Only card networks are authorized to act as TSPs under the previous regime. Card issuers can now tokenize and de-tokenize card data by offering tokenization services.
According to the circular, tokenization of card data would require clients' explicit authorization and confirmation by the card issuer using an Additional Factor of Authentication [AFA]. When a card is renewed or replaced, the card issuer must obtain the cardholder’s permission to link the new card to the same merchants as the previous card.
Governance Mechanism And Anti-Money Laundering Objectives
The governance of PAs and PGs must meet the standards for authorization and capital, according to RBI regulations. The Chief General Manager, Department of Payment and Settlement Systems [DPSS], and the RBI Central Office in Mumbai must be notified in writing within 15 days of any takeover or management change of a non-banking PA.
The letter must include all relevant information, including a ‘declaration and undertaking’ from each new director, if applicable. RBI will assess the management’s status and, if necessary, may impose reasonable restrictions on such changes.
It is required that they “appoint a Nodal Officer responsible for regulatory and customer grievance handling functions”, as well as adopt policies for handling complaints and dispute resolution processes for processing refunds following the RBI’s Turn Around Time [TAT] regulations.
The entities shall follow the Master Directions - Know Your Customer Directions to fulfil the objective of anti-money laundering and negate the financing of terrorism. The Prevention of Money Laundering Act, 2002 is also applicable.
Merchant On-Boarding
Participating merchants/digital wallets must either interface directly with card networks or use token service providers to create a secure environment for card tokens. These token service providers must be certified by the card networking systems and the Payment Card Industry-Data Security Standard [PCI-DSS]. Banks and card networks must incentivize digital firms to support tokenized transactions.

The terms and conditions of the service – along with the TAT for returns and refunds – must be clearly stated on the merchant's website.
Cards and other sensitive data will not be saved on the merchant's website. A security audit of the merchant can be performed as needed to guarantee compliance. The customer's data must be secured under the contract with the merchant.
Card tokenization could help online businesses in sectors such as meal ordering, travel and online shopping if the RBI allows new-use cases authorisations such as 'card-on-file' over time. Financial applications such as Jio Pay, GooglePay and PayTM will have to integrate with merchant apps as they enable card tokenization until the RBI issues further guidelines and/or any other necessary permissions.
Settlement and Escrow Account Management
As per Section 23A of the Payment and Settlement Systems Act, non-bank PAs must keep the funds they collect in an escrow account with a certified commercial bank. PA operations are deemed "designated payment systems" to keep an escrow account.
Security and Risk Management Framework
The token-mapping procedure makes use of the card data vault, which serves as a central repository for Permanent Account Numbers [PANs] and tokens. Wherever PAN data is stored, it must be managed and protected in line with Payment Card Industry Data Security Standard [PCI DSS] requirements. The data vault is often the most enticing target for attackers because it contains PANs in addition to tokens. If the data vault is breached, the entire tokenization system may be jeopardized, necessitating additional security precautions beyond those mandated by PCI DSS.
PAs & PGs must develop a tracking plan, respond to, and follow up on cyber security incidents and breaches, all of which must be immediately notified to the RBI's Office in Mumbai. They must also alert the CERT-In [Indian Computer Emergency Response Team].
Remarks
The RBI circular's requirements make it easier to deregister tokens. Card issuers must allow users to review the list of businesses for whom the CoFT has been selected and deregister the token using mobile apps, internet banking, etc. Retailers must allow cardholders to deregister the token. The RBI has stated that tokenization services will not affect the convenience of customers' transactions.
Since Indian Data Protection laws are still relatively new, the RBI's tokenisation procedures for data security are required to protect consumers' sensitive data. However, for a tokenisation infrastructure to function properly, various participants in the banking system would need to collaborate, which may offer some challenges.
[1] Reserve Bank of India, FAQs- Payment System-Tokenisation, https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=2917
[2] Reserve Bank of India, RBI/2018-19/103 DPSS.CO.PD No.1463/02.14.003/2018-19, "*Tokenisation – Card transactions*", https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=1144
[3] Reserve Bank of India, RBI/2022-23/77

CO.DPSS.POLC.No.S-567/02-14-003/2022-23, “*Restriction on storage of actual card data*”, 23 December 2021, https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=12345
Contributed by Abhilasha SG, Associate & Dhaval Bothra, Banking