Retail Liabilities
Customer Relationship & Business Development Department

Central Office, 82-83, 8th Floor, Maker Towers, Cuffe Parade, Colaba, Mumbai-400 005

Product Information on Tokenisation on Cards Transactions

As per the regulatory guidelines of RBI, with effect from 01st July, 2022, Banks introduce tokenization facility for all the card users of both Debit and Credit card holders of RuPay/VISA/Master card to enhance online transaction security.

Under Tokenisation facility, neither the Payment Aggregators (PAs) nor the Merchants can store customer card credentials within their data base w.e.f. July 01, 2022.

All the Payment Aggregators (PAs)/Payment Gateway acquirers should replace the stored card on file with tokens and the basic purpose of tokenisation is to enhance security for digital transactions.

No charge will be recovered from customers for availing tokenization facility. This will help in achieving secured customer service excellence.

- Tokenization facility is an additional feature to our Debit and Credit card holders provided by the card networks RuPay/VISA/Master card.
- Tokenisation will allow a seamless and convenient transaction experience with heightened data security.
- Tokenisation facility will help millions of customers maintain security of their card financial data for online transactions and the card details will now completely safe and secure.
- Based on the set of guidelines that have been mandated by the RBI, sensitive customer information is to be stored in the form of an encrypted "token" to help secure transactions, so that it cannot be hacked or read by any other person.
- These tokens will then allow payments to be processed without disclosing the customer details or allowing the payment intermediaries to store customer data that could breach security and privacy.
- Tokenisation will enhance safety and further strengthen the digital payments ecosystem in the country. In addition to enhancing security, tokenization will also help in reducing friction in the payment process by providing a faster check out experience to customers. It is a safe transaction experience and for convenience of the customers.

About Card on File Tokenisation (CoFT):

- Card on File Tokenisation refers to neither the authorized payment aggregators (PAs) and Merchants on-boarded shall store customer card credentials instead a card on file, or stored credentials, is the card information stored by a merchant, payment gateway, payment aggregator or digital wallet to process future transactions to enable card holders to benefit from the security of tokenized card transactions in a safe, secure and in a convenient mode.
- As per the guidelines of RBI, **for the purpose of CoFT,** Card tokenization refers to replacement of actual card details with an unique alternate code called "token" which **shall be unique for a combination of card, token requestor and merchant.**
- If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then Additional Factor Authentication (AFA) may be combined.
- For transaction tracking and / or reconciliation purposes, entities can store limited data i.e., last 4 digits of actual card number and card issuer's name – in compliance with the applicable standards.
- The list of merchants in respect of whom the CoFT has been opted by the cardholder to de-register any such token, a facility shall be provided through one or more of the following channels – mobile application, internet banking, interactive voice response (IVR) and branches.
- Whenever a card is renewed or replaced, the card issuer shall seek explicit consent of the cardholder for linking it with the merchants with whom he/she had earlier registered the card.
- The Token Service Provider (TSP) shall put in place a mechanism to ensure that the transaction request has originated from the merchant and the token requestor with whom the token is associated.

---@@@---