

# Tokenisation of credit and debit cards

October 4, 2022

**In news**– From October 1st, 2022, the Reserve Bank of India's card-on-file(CoF) tokenisation norms have kicked in, which aim at improved safety and security of card transactions.

## **What are the new norms?**

- Now, for any purchases done online or through mobile apps, merchants, payment aggregators and payment gateways will not be able to save crucial customer credit and debit card details such as three-digit CVV and expiry date.
- In September 2021, the RBI prohibited merchants from storing customer card details on their servers with effect from January 1, 2022, and mandated the adoption of card-on-file (CoF) tokenisation as an alternative.

## **What is tokenisation?**

- Tokenisation refers to the replacement of actual card details with a unique alternate code called the 'token', which shall be unique for a combination of card, token requester, (i.e. the entity which accepts requests from the customer for tokenisation of a card and passes it on to the card network to issue a corresponding token) and the device.
- A debit or credit card holder can get the card tokenised by initiating a request on the app provided by the token requester.
- The token requester will forward the request to the card network which, with the consent of the card issuer, will issue a token corresponding to the combination of the card, the token requester, and the device.
- In case of an online transaction, instead of card

details, a unique token will be stored on the server.

- The merchant or transaction platform sends out a message to Visa or Mastercard or a payment gateway, who asks for a token against that card number and will then pass it on to the bank for allowing the transaction.
- The customer will not be charged for availing the tokenisation service.
- Earlier, the facility for card tokenisation was available only for mobile phones and tablets of interested card holders.
- **Subsequently, with an uptick in tokenisation volume, the RBI decided to extend the scope of tokenisation to include consumer devices – laptops, desktops, wearables (wrist watches, bands, etc.) and Internet of Things (IoT) devices.**
- **A tokenised card transaction is considered safer** as the actual card details are not shared with the merchant during transaction processing.
- Actual card data, token and other relevant details are stored in a secure mode by the authorised card networks.
- **The token requestor cannot store Primary Account Number (PAN), or any other card details.**
- **Card networks are** also mandated to get the token requester certified for safety and security that conform to international best practices/globally accepted standards.
- **Tokenisation can be performed only by the authorised card network** and recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only.
- Adequate safeguards have to be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network.