# Ensuring safety through tokenization



**(Mains GS 3 : Indian Economy and issues relating to planning, mobilization, of resources, growth, development and employment.)**

**Context:**

- Many merchants and e-commerce entities force customers to store debit or credit card details, which increases the risk of card data being stolen.
- This can be avoided now with the Reserve Bank of India allowing tokenisation of cards while making payments.

**The tokenisation:**

- According to RBI, it refers to replacement of card details with an alternative code called a ‘token’, which is unique for a combination of card, token requestor (the entity that accepts a request from the customer for tokenisation of a card and passes it on to the card network to issue a token) and the device.
- It reduces the chances of fraud arising from sharing card details.
- The token is used to perform contactless card transactions at point-of-sale (PoS) terminals and QR code payments.

**Tokenisation of Card-on-File:**

- The RBI has also extended tokenisation of Card-on-File (CoF) transactions (where card details used to be stored by merchants) and directed the merchants not to store card details in their systems from January 1, 2022.
- A CoF transaction is one in which a cardholder has authorised a merchant to store his or her Mastercard or Visa payment details, and to bill the stored account.
- E-commerce companies and airlines and supermarket chains often store card details.

- With effect from January 1, 2022, no entity in the card transaction or payment chain, other than the card issuers and card networks, should store the actual card data and any such data stored previously will be purged.

**Working of tokenisation:**

- The cardholder can get the card tokenised by initiating a request on the app provided by the token requestor.
- The token requestor 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 requestor, and the device.
- Tokenisation has been allowed through mobile phones or tablets for all use cases and channels like contactless card transactions, payments through QR codes and apps.
- The tokens are generated by companies like Visa and MasterCard, which act like Token Service Providers (TSPs), and they provide the tokens to mobile payment or e-commerce platforms so that they can be used during transactions instead of the customer's credit card details.

**Safeguarding transaction:**

- When users enter their card details into a virtual wallet like Google Pay or PhonePe, these platforms ask one of these TSPs for a token.
- The TSPs will first request verification of the data from the customer's bank.
- When the data has been verified, a code is generated and sent to the user's device. Once the unique token has been generated, it remains irreversibly linked to the customer's device and cannot be replaced.
- Thus, each time a customer uses his or her device to make a payment, the platform will be able to authorise the transaction by simply sharing the token, without having to reveal the customer's true data.
- Tokens can be generated to safeguard payments in mobile wallets and physical or online stores like Amazon.

**Who can tokenise cards:**

- The RBI has permitted card issuers to act as TSPs, which will offer tokenisation services only for cards issued by or affiliated to them.
- The ability to tokenise and de-tokenise card data will be with the same TSP.
- Tokenisation of card data will be done with explicit customer consent requiring Additional Factor of Authentication (AFA) validation by the card issuer.

**Stakeholders involved:**

- Normally, in a tokenised card transaction, the stakeholders involved are the merchant, the merchant's acquirer, card payment network, token requestor, issuer and customer.

- The registration for a tokenisation request is done only with explicit customer consent through AFA, and not by way of a forced, default or automatic selection of check box, radio button, etc.
- Customers will also be given the choice of selecting the use case and setting up limits. Customers have the option to set and modify per-transaction and daily transaction limits for tokenised card transactions.

**process after tokenisation:**

- According to the RBI, for transaction tracking and reconciliation, entities can store limited data — last four digits of actual card number and card issuer's name — in compliance with applicable standards.
- Actual card data, token and other relevant details are stored in a secure mode by authorised card networks.
- The token requestor cannot store the card number, or any other card detail. Card networks are also mandated to get the token requestor certified for security conforming to international best practices / globally accepted standards.
- A customer can choose whether or not to let his or her card tokenised.
- Besides, the card issuer should also give the cardholder the facility to view the list of merchants for whom he or she has opted for CoF transactions, and to de-register any such token.

**Reasons RBI going for tokenisation:**

- Citing convenience and comfort for users while undertaking card transactions online, many entities involved in the card transactions store actual card details, which is CoF.
- In fact, some merchants force their customers to store card details.
- Availability of such details with a large number of merchants substantially increases the risk of card data being stolen.
- In the recent past, there have been incidents where card data stored by some merchants have been compromised or leaked.
- Any leakage of CoF data can have serious repercussions because many jurisdictions do not require an AFA for card transactions.
- Stolen card data can also be used to perpetrate frauds within India through social engineering techniques, the RBI said.