Tokenisation of Cards in India

For Prelims: Reserve Bank of India (RBI), Tokenisation, Sensitive Data, Card-on-File system, Digital Payments.

For Mains: Significance of Tokenisation.

Why in News?

Recently, the **Reserve Bank of India (RBI)** has made tokenisation mandatory for all credit and debit cards used in online, point-of-sale, and in-app transactions.

- The customer will not be charged for availing the tokenisation service.

What is Tokenisation?

- It 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.

What was the Need for Tokenisation?

- **Vulnerability of Sensitive Data**: E-commerce giants like Amazon, Myntra, Flipkart, Bigbasket, etc., save sensitive card details with them like card number, expiration date, and CVV get stored in these companies' databases.
  - But if the databases get hacked, it poses a real problem as all the card data will become easily accessible.
- **Rise of Digital Fraud:** The **COVID-19** pandemic has pushed drastic changes into the digital economy. With more and more customers and merchants adapting to **digital payments,** it is now more important than ever to tighten security.
  - With an average of 6 billion transactions happening every month, fraud could also grow proportionally if not taken care of.
  - This fraud can be a huge threat to the entire country's financial system. From 2019 to 2020, **card fraud has increased by 14% Compounded Annual Growth Rate (CAGR), while in the last three years, it has increased by 34%.**
- **Outdated Present System:** The current **Card-on-File system (CoF)** can be easily breached, and the data can be stolen. So, to take care of the security concerns, RBI has come up with the Tokenization system, which guarantees that the customers' details cannot be breached and cannot be misused by anybody.
  - A CoF transaction is a transaction where a cardholder has authorised a merchant to store the cardholder's Mastercard or Visa payment details.

Who can Offer Tokenisation Services?

- **Authorised Card Networks:** Tokenisation can be performed only by the **authorised card network** and recovery of the original **Primary Account Number (PAN)** should be feasible for the authorised card network only.
    - Further, adequate safeguards have to be put in place to **ensure that PAN and other sensitive data cannot be found from the token and vice versa,** by anyone except the card network. RBI has emphasised that the integrity of the token generation process has to be ensured at all times.

What are the Benefits of Tokenisation?

- A tokenised card transaction is considered safer as the actual **card details are not shared with the merchant during transaction processing.** Real card data, tokens and other relevant information are stored securely 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 conforms to international best practices/globally accepted standards.
- Tokenization paves the way for **advanced innovations in the payment ecosystem.** It has become the cornerstone for payments, whether in-store, online or through mobile wallets.
- Strengthens trust between customers and businesses.
- Reduces the level of red tape for businesses.
- Creates an ecosystem of smoother and safer payment experiences for all parties involved.

What is the Status of Card Payments in India?

- As per RBI's annual report for 2021-22, payment transactions carried out through credit cards increased by 27% to 223.99 crores in volume terms and 54.3% to 9.72 lakh in value terms during 2021-22.
- Till July (2022), the number of credit cards issued stood at around 8 crores, and debit cards in the system were 92.81 crores.

UPSC Civil Services Examination Previous Year Question (PYQ)

Prelims

Q. Consider the following statements: (2019)

The Reserve Bank of India's recent directives relating to 'Storage of Payment System Data, popularly known as data diktat, command the payment system providers that

1. they shall ensure that entire data relating to payment systems operated by them are stored in a system only in India
2. they shall ensure that the systems are owned and operated by public sector enterprises
3. they shall submit the consolidated system audit report to the Comptroller and Auditor General of India by the end of the calendar year.

Which of the statements given above is/are correct?

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (a)

Exp:

- In order to have unfettered access to all payment data for supervisory purposes, the Reserve Bank of India had directed that all the system providers shall ensure that the **entire data relating to**

payment systems operated are stored in a system only in India. This data includes the full end-to-end transaction details/ information collected/carried/processed as part of the message/payment instruction. **Hence, statement 1 is correct.**

- No provision regarding the ownership and operation of the systems by public sector enterprises has been provided. **Hence, statement 2 is not correct.**
- RBI had also directed payment system providers to submit the System Audit Report (SAR) with an audit mandatorily conducted by CERT-IN empanelled auditors. **Hence, statement 3 is not correct. Therefore, option (a) is the correct answer.**

Source: IE