Compliance requirements for Card Tokenization

What is tokenization and how does it help?

Tokenization is the process where card details are replaced with a unique token which can't be reversed. This leads to enhanced security in the payment journey and protects customer data thus enabling secure, faster payment experience and reduced frauds.

As per the RBI guidelines on Tokenization – Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services, w.e.f. 1st October, 2022, merchants will not be allowed to store your card number, CVV and expiry date for processing online transactions. Any existing details that were saved by merchants will be deleted.

Following RBI guidelines govern saving of cards in India (henceforth, CofT aka Card on File Tokenization)

1. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12573&Mode=0
2. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11449&Mode=0
3. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0
4. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12345&Mode=0
5. https://rbi.org.in/Scripts/FAQView.aspx?Id=129

Important points to keep in mind:

1. Card on File Data such as 16-digit card number, expiry date/month and CVV can be stored by only two entities – the card issuing bank and the card issuing network.
2. Limited data can be stored by non-payment entities (Bank Name, Last 4 digits of card)
3. To provide saved card transaction experience, merchants must create a Card on File Token which is the most secure manner.
4. Every token must be created with **EXPLICIT customer consent.**
5. Every token must be created with Additional Factor of Authentication
    a. Verbatim – RBI: "2. If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then AFA validation may be combined."
6. A token will be unique to the customers card details, customer credentials such as mobile number etc and merchant.

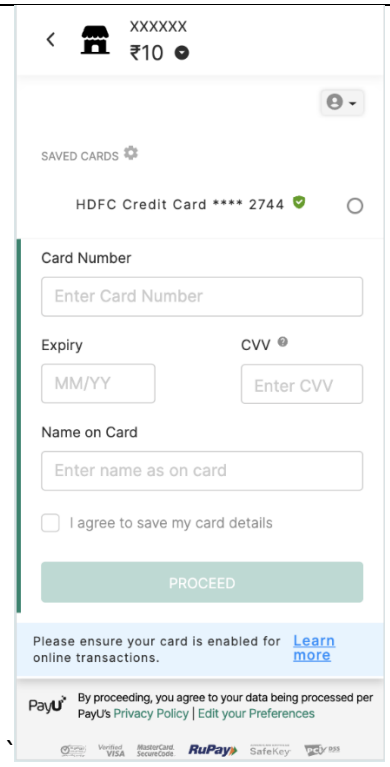
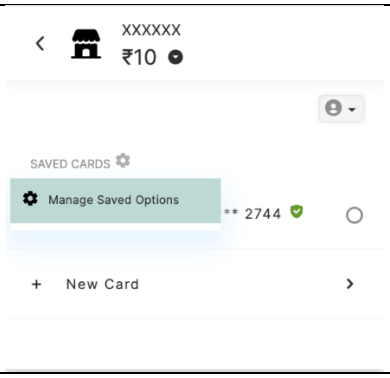
Impact on your business:

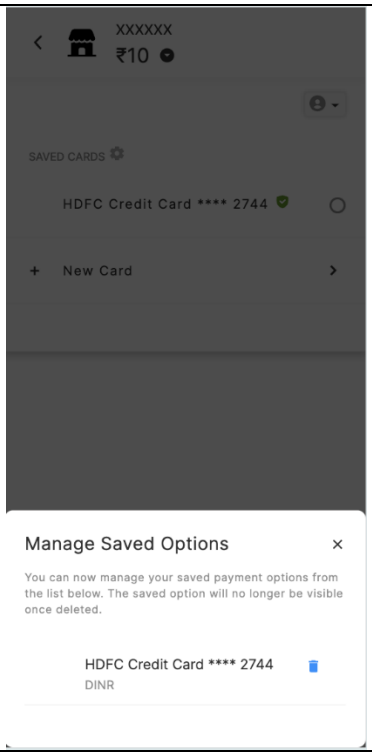
1. To provide saved card payment experience to the customer you must show the option to save card as per RBI guidelines and capture user's explicit consent for the purpose of tokenising the card.
   Default behaviour, if the customer is not interested to save the card, then there would be no tokenization.

2. If you have multiple line of businesses, which are separate in terms of legal and consumer facing entities, please ensure that the tokens are created for each business separately. **Example**: If merchant A has 3 different line of business LOB1, LOB2 & LOB3 then as per tokenization norms whenever a customer with his/her card details navigates to this line of business and opts to save the card and completes the AFA i.e. OTP authentication then different tokens will be created
3. Ensure that you keep a log of consent being given by the customer and the AFA of transaction been done and maintained for audit purposes
4. Ensure that you are giving customers an option to delete the token. RBI mandates both the issuer and the merchant to allow customers to withdraw consent and deregister the token

PayU's support:

1) If you are using PayU powered checkout, we already comply with every facet of RBI regulations.

Explicit user consent	
Manage Cards	

Delete Card	

Note: If you have a seamless integration – You call PayU's APIs for tokenization

1. There are two new fields added in the save card API. Please ensure you pass on the consent value and Authentication Status. We recommend you send these details when calling our Save Card API (https://docs.payu.in/reference/save_card_api).
    a. var10: is Additional Factor Authenticated
    b. var11: Is the consent received from the customer
2. Please integrate with the lifecycle management APIs
    a. These APIs will inform you if the card token has expired or deleted, if the underlying card has expired or if the customer has deleted from the bank portal
    b. This will help reduce errors when you are trying to initiate a transaction and it fails due to the token not being active.
    c. The API details can be found here: https://docs.payu.in/docs/api-notifications-for-tokenization