# Card-on-File Tokenization – Can RBI Bridge The Gap?

**RBI mandates Card-on-File Tokenization ("CoFT") framework for Payment Aggregators and Payment Gateways. In this article, I expand on what it is and how it affects merchants and the consumers.**

In August 2021, the Reserve Bank of India ("**RBI**") vide its notification issued a directive that any entity that is not a card network (such as MasterCard, Visa etc.) or an issuing bank, must not store and discard any customer card details stored by them in the past, irrespective of whether such storage was in compliance with the Payment Card Industry Data Security Standard (PCI-DSS). When the RBI published the said notification, there was explicit dissent from online merchants (i.e. anyone that accepts digital payments online) since it pre-emptively creates reliance on third-parties such as card networks to execute transactions.

According to the new digital payments guidelines, RBI has prohibited storage of card info locally with merchants and permitted card networks/ aggregators to offer card tokenisation service as Token Service Providers ("**TSPs**").

Tokenisation is the process of masking actual credit or debit card details with an encrypted alternate alias of numbers, referred to as a 'token', which will be a unique combination for every token requestor and device. A tokenised card transaction is considered safer as the actual card details are not shared with the merchant during transaction processing, since the original card details mapped with the pseudo token number only exists with TSPs. The token is then used to perform online transactions with merchants, food delivery platforms and QR code payments tied with a debit/ credit card. This enables payments to be processed without exposing any sensitive account details that can potentially breach security and privacy of the consumers in an event of a data breach.

A cardholder can get their debit/ credit card tokenised by initiating a request on the application by the online merchant or the bank. The token requestor will then forward the request to the card network which, with the consent of the card issuing bank, will issue a token corresponding to the combination of the card, the token requestor, and the device. This mechanism allows merchants to access and to store the unique token reference against the card holder details, instead of collecting entire card details in verbatim, minimising vulnerable points in the system. This precautionary move by the RBI sets a firm precedent in demonstrating regulatory foresight to keep up with global security standards, and paves the path for secure, seamless payments.

According to the RBI, for transaction tracking and reconciliation, merchants can only store limited data such as last four digits of actual card number and card issuer's name for reference. Actual card data and other relevant details will be stored in a secure mode in the token by authorised card networks. Card networks are also mandated to get the token

requestor certified for security conforming to international best practices/ globally accepted standards.

However, the primary challenge in card tokenisation is for merchants while accessing card data, which in turn has an impact on merchants providing smooth service to their customers as card information enables the merchants handling any use case scenarios like recurring e-mandates in equated monthly instalments and subscription based services, EMI options, post-transaction activity inter alia providing prompt refunds, reward/ loyalty programmes, dispute handling and preventing fraud in an impactful and efficient manner. Although the move is a progressive one, but the general laxity and unpreparedness of the industry to provide enabling framework has left merchants scrambling with major technology integration challenges, with no infrastructure provided by the RBI. With only a few banks and merchants compliant with the mandate, the December deadline was rather a cursory one, which was not enforced by the RBI. Now, as 2021 has come to an end, another deadline has emerged over the card payment ecosystem in India as RBI has shifted the deadline by six more months from the earlier December, 2021 to June, 2022.

While RBI's legislative intent to protect consumer interest is to be commended, any disruptions in service and challenges on ground pertain to implementation as opposed to pushing the legislation on paper as demonstrated by the contrasting execution. Unless a fully functional framework of tokenization, has been systematically implemented in a tiered manner starting from TSPs to merchants, merchants won't be able to continue to serve customers without asking the consumer to input full card details every single time. While major card networks like Visa, Mastercard and Amex are catching up, less popular card networks and merchants such as Rupay, JioPay and Paytm have partnered with National Payments Corporation of India (NPCI) to follow compliance.

In foresight, this puts merchants in a conundrum to serve customers seamlessly or to hamper the continuity of their operations relying on external third parties (such as card networks and/ or banks) for compliance. Disruptions of this nature corrodes consumer trust in digital payments and reverses consumer habits back towards cash payments, undoing years of work to encourage digitisation. If tokenisation is not ready by June, 2022, then merchants can either continue serving their customers and be non-compliant or comply and lose the ability to perform their operations smoothly.

It is indeed a very progressive move by the RBI following numerous data breaches and an absence of a robust data privacy system in India. The legislation seems very promising in avoiding sensitive data leaks, reducing system vulnerabilities and ensuring data privacy and is a step in the right direction. With that being said, the merchants lack the ability to influence any readiness on to the highly interdependent ecosystem. The lack of chronological planning coupled with operational challenges has left merchants aggrieved and dissatisfied as only card networks are responsible for developing such infrastructure, leaving merchants on the last leg as they are forced to delete all CoFT data they have collected over the years. RBI has delegated a rather legislative function of systematic execution and developing a vital digital infrastructure to bridge the gap between policy and practicality. As time runs out with another deadline

looming over, RBI must ensure compliance readiness well in advance by working with all the stakeholders parallelly and in a symmetrical manner, starting with merchants to ensure a smoother transition.