



## Request for Extension of Timelines for Merchants for Implementing Tokenization Solutions

---

The Internet and Mobile Association of India (IAMAI) is a not-for-profit industry body dedicated to representing the entire gamut of digital businesses in India. IAMAI's membership includes sectors such as e-commerce, digital advertising, digital entertainment, digital payments, digital gaming, EdTech and Healthtech among others. These sectors encompass varied digital merchants across different sectors and hence, to be a common voice of these merchants, we have formed a merchants committee under IAMAI. This committee would represent the digital merchant's ecosystem in the country. The vision of this committee is for now limited to ensuring smooth and secure functioning of the payments related services of merchants. This committee could be the single point of contact for RBI to reach out to in case of any merchant consultations required for digital/online merchants.

As we move towards achieving the goal of becoming a cashless economy, it is important to have safe and secure digital payments. In this regard, we on behalf of the entire industry and the users, welcome the Reserve Bank of India (RBI)'s intent in protecting consumers when making payments via digital means. However, we would also like to share our members' thoughts and concerns in respect of placing storage restrictions on customer card data *vide* the '[Guidelines on Regulation of Payment Aggregators and Payment Gateways](#)' dated 17 March 2020, read with the clarification and directive issued thereunder (**PA/PG Guidelines**). We also commend the RBI's initiative of offering stakeholders within the payments industry with alternative solutions to these restrictions through its [Card-on-File Tokenisation Services](#) circular (**CoFT Services Circular**).

After assessing the internal readiness of the banks, card schemes and technology service providers, we believe merchants would require additional time to adhere to the card data storage limitations and data purging obligations; this is because as on date, card networks and banks are not ready, and merchants are inevitably dependent on other regulated entities such as card networks, banks etc., for compliance of their own obligations under the PA/PG Guidelines and CoFT Services Circular. ***We humbly request the RBI to extend timelines for merchants for implementing tokenization solutions by 6 months, from the date when card networks and banks complete their readiness, keeping in mind their inevitable dependency on the other regulated entities in the payment ecosystem.***

IAMAI's recommendations below have attempted to best capture the challenges the September 7<sup>th</sup> circular would pose to Merchants. We request RBI to integrate the Merchant community's perspective in their decision-making process.

### IAMAI Submission

#### 1. Tiered timelines for implementation & prioritized compliance for Banks

The requirement to delete all card storage data is indubitably intended to protect the consumer, however, to transition from the current system to a model which is as convenient but more secure



would require enough room for merchants to function under the current system, till an alternative is adequately usable.

#### **Ecosystem Readiness:**

For tokenization to be implemented effectively requires a sequential process of compliance from across the value chain of the payment ecosystem. This means that once card networks create the base infrastructure, banks need to create theirs and integrate with the card network infrastructure. Thereafter (and not before or during), merchants integrate with the now combined (card network + bank) system, thereby becoming part of the solution that allows customers to transact using digital payments in a safe and friction-free manner.

The need to have a tiered time line for adherence is imperative as that banks' compliance with the tokenization circular is discretionary. However, without banks' wholehearted participation, the card networks' solution is irrelevant and merchants' compliance is nearly impossible. Therefore, the bank's compliance /readiness as per the Tokenization Circular cannot be optional as a crucial part of a payment processing hinges on the Bank's readiness for ecommerce/ online merchants. We appreciate that payment processing is merely a part of the Bank's P&L accounts, since it provides other offline banking services, loan disbursal etc., while for an ecommerce /online entity, which is dependent on the Bank's readiness to process payments against its business transactions, it will become a business continuity risk if the Bank is not ready with the tokenization solution. Thus, the RBI should prescribe a definition for "system readiness" for the bank and card networks, and only when such definition is fulfilled that merchants can be onboarded, otherwise the ecosystem will continue to face challenges. We have learnt from the recent experience during the implementation of the e-Mandate requirement, where the banks and networks did not prioritize preparedness, it became a question of business continuity for many merchants due to the ripple effect of non-readiness. For this reason, we urge banks to comply with the tokenization direction on priority. We also request the RBI to monitor banks' compliance status closely which should be reported transparently to the merchants to ensure their timely readiness.

In any circumstance, technical readiness is a function of the following - conceptualising, developing and designing infrastructure, then testing it, then fixing any bugs/ gaps, then completing any integration in an interdependent ecosystem, and finally rolling it out to the customer. In the context of the payment's ecosystem, this process needs to be completed by every participant in the payments chain - i.e. card schemes, banks, payment processors and merchants. Until the upstream participants share stable state documentation (i.e. final APIs) with the merchants, the merchants are technically incapable of even commencing building the relevant infrastructure at their end. Even when merchants complete building the infrastructure, the comprehensive solution will be some ways away from being ready to be rolled out to consumers - it will require testing, fixing the gaps and only after that will it truly be a ready tokenization solution.

This makes compliance to the new requirements (of no card storage) by December 31<sup>st</sup> a huge challenge for merchants, since tokenization is an alternative to card storage. IAMAI would like to

recommend a tiered timeline for adherence to the new system. This would mean that the 31<sup>st</sup> December deadline only applies to banks and card networks. Once those compliances have been met, **merchants must be allowed a further 6 months** for testing, integration, moving from legacy rails to the new solution, and offer it to customers. **It is crucial for RBI to continuously monitor the state of readiness of card networks and banks**, and ensure that **compliance requirements for merchants (including data purging etc.) are triggered only after the remaining ecosystem (i.e. card networks and banks) have confirmed they are ready**, else there will be a complete breakdown of merchants' ability to serve customers.

Also, if the requirement to purge CoF data is enforced without giving merchants 6 months after attaining ecosystem readiness, customers experience and card payments will be significantly disrupted. The enforcement of these requirements before a holistic adoption of tokenization would mean that consumers would have to manually enter card details for every purchase. This is in conflict with the government's goal of increasing ease of doing business, especially since the consumer would directly be impacted by this compliance.

Aside from a complete breakdown in the Card payments system, improper implementation also poses serious threats to the Digital Economy. Without ecosystem readiness, merchants will not be able to provide life cycle management services including but not limited to refunds, grievance redressal, rewards or offers to consumers who may not have initiated the tokenization process or might not be able to due to ecosystem unreadiness.

#### **Battling Fraud:**

Merchants have put in place robust risk assessment frameworks to control frauds on their platforms, which have been built in collaboration with banks and payment system operators. Without card data or CoF tokenization, merchants cannot engage in such crucial fraud prevention measures, which will have a huge impact on consumer confidence and the adoption of digital payments.

#### **Recurring Payments:**

Consumers will see increased friction in acquiring subscription-based services that require storage of card data or tokenized card data to bill consumers on a recurring basis. Consumers expect subscription services to be provided in a seamless manner and provide merchants with consent to store their card information and charge their cards until they cancel the service in accordance with RBI regulations. Moreover, consumers can seamlessly cancel their subscriptions digitally at any time. Without Card data or CoF Tokenization, merchants will need to ask for card information every billing cycle or create separate tokens with each issuer (by collecting card data from the consumer more than once) which will impact the consumer experience significantly.

## **2. Storage of BIN Ranges:**

The PA/PG guidelines permit PA and merchants to store limited data for tracking purposes, however, do not define the scope of limited data. The RBI circular dated 7<sup>th</sup> September further



defined limited data as the last four digits of the card and the name of the cardholder. From a technical perspective this is challenging, as this information alone is inadequate to service customers. Keeping consumer interest in mind, IAMAI would like to recommend permitting the storage of BIN ranges as well.

BIN ranges are the first few digits of a card which are publicly available and indicate the bank and card network of a given card. Without BIN ranges, merchants will be unable to support customers with requests for subscription, refunds, cancellations, fraud risk mitigation, any other customer service requirements etc.

Further, to accelerate digital payment adoption, different card issuers run customer incentive offers from time to time. These offers work(ed) on BIN identification. Today ecommerce merchants and banks use this BIN to run bank discount campaigns, reconciliation, identification of users that are facing downtime and other errors. With the advent of tokenization, since merchants would not be able to identify the BINs, they will also be unable to run such campaigns which would significantly impact digital payment adoption. Therefore, we request the RBI to clarify and allow merchants to store BINs along with the last four digits of the card number.

There is a considerable amount of development required in the merchant downstream system to identify Token Ranges and apply MDR as per revised logic. Merchants will also require file formats, frequency and exchange mechanism of BIN range for MDR computation.

### 3. Consent for Renewed and Replaced Cards:

The RBI notification also mandates fresh consent requirements for renewed or replaced cards. This significantly complicates the management of the life cycle of tokens. The requirement to refresh consent disrupts the advantage tokens have over traditional card storage, in that it no longer allows tokens to automatically refresh with no interruption to scheduled payments and no discontinuation of services upon card renewal.

IAMAI believes the customer should have the right to take advantage of the enhanced convenience offered by tokenization technology and not be required to provide consent each time a card is renewed/replaced (delayed consent may lead to disruption of services).

### 4. Seamless Migration:

Card networks have been asking for Additional Factor Authentication for the migration of cards to the new solution from legacy systems. This would be counterproductive and only serve to complicate the process of migration, particularly considering that Merchants have in place customer consent from the time they sought the customer's card information in the first place. IAMAI believes there is no requirement for the same and request card networks to facilitate seamless migration.

## 5. Use of same token within same entity and in case of 'parent app'

Currently in the market, there are multiple customer payment journeys built by the merchants in their application under the same legal entity name. Merchant should be allowed to use same token for all possible journeys without requesting for additional token. We believe, this will reduce token management overheads for the merchant substantially and do away the requirement of saving card for every journey in same application. We also insist that merchants should be allowed to use same token for different legal entities in case of super app construct.

## 6. Clarification on Transactions Processing

We request additional clarification for following points in the light of compliance by merchant ecosystem with the proposed notification of RBI.

- **EMI Transaction Processing** - This feature brings in lot of convenience to customers for large value transaction purchases and ambiguity in tackling will disrupt affordability segment. In the current process, PG/PA shares offline file containing clear card details with issuing banks for EMI conversion but with new guidelines, PA/PG will no longer be storing card details. Therefore, clarity is required from Networks and issuing banks on handling such transactions.
- **Offer Transactions Processing** - Few networks have clarified to use PAR (Payment Account Reference) for performing dedupe checks on Offers and can be fetched irrespective of Card Tokenization. But clarification is awaited from some of the Networks in this regard where PAR comes only in tokenization response. We request more clarity on the flow for non-saved card transaction journey. At the same time, issuer has to update whether they will be able to identify card with last 4 Digit and Token Reference for posting Deferred Cashback.

## 7. Clarification on applicability of Guidelines

The Guidelines and related circulars referred above direct that no entity in the payment chain other than Card Issuers and/ or Card Networks shall store the actual card data. The payments ecosystem including merchants and customers would be pleased to receive a clarification on the ambit of the card-based transactions covered by the said Guidelines and notifications in this regard:

- Do the guideline and related circulars apply to only Card not present Transactions? Or does it also include physical store/ merchant establishment and POS based transactions?
- The industry is proceeding with the understanding that international card transactions undertaken by Indian card-holders with overseas merchants via card acquirers with no presence in India without connection or relationship with any regulated entities in India are outside the scope of both; extant regulations of Payment Aggregators/Payment Gateways and guidelines on card tokenization.

## 8. Allow the storage of card details of guest users

Several customers conduct online transactions as a guest without registering on the merchant portal/ website. However, refunds to such guest customers if applicable, would be a challenge, in case the merchant is unable to store the actual card data as the merchants would not know which payment instrument to be refunded securely. Thereby, putting the customer at a major disadvantage. Therefore, unregistered customers on merchant portal/ website or app may kindly be allowed to pay and allow storage of their card details with merchant portals/websites or apps till such time a refund period offered by a merchant is active i.e, 15 days or a month depending on the valid period of refund offered by the merchant.

## Conclusion

IAMAI would once again like to congratulate the RBI on its vision to protect consumers, and for putting the interests and data privacy of consumers first. We firmly believe that in a rapidly digitizing India, this will add an additional level of trust and safety to help bring more businesses and consumers online. However, to achieve this with minimal consumer and business disruption and to the full extent of the technology's potential, taking the merchant perspective into account is extremely necessary.

For a seamless implementation of the Card-on-file tokenization, IAMAI would like to submit the following suggestions to RBI from the perspective of merchants:

1. **Mandate and ensure priority compliance by RBI's regulated entities** (like card networks and banks) **by the stated deadline of 31 December 2021** to ensure "system readiness". Once these entities are ready, **permit tiered implementation timelines by allowing merchants another 6 months to complete their compliance, including the timeline for purging of data.** It is crucial that Merchants are allowed to store CoF data for at least 6 months after card networks and banks are ready, to avoid huge disruptions in payments to online businesses.
2. Permit merchants to store BIN ranges.
3. Remove fresh consent requirements for renewed/ replaced cards.
4. Facilitate seamless migration of cards from the legacy to new systems.
5. Issue clarifications on EMI payments and offer transaction processing
6. Issue clarification on applicability of guidelines w.r.t physical stores/ POS based transactions and international card transactions.
7. Allow the storage of card details of guest users for making refunds.