Card-on-file and recurring transactions: Impact of regulatory guidelines

April 2021

Foreword

Dear readers,

It is my pleasure to bring to you the latest edition of our payments newsletter. In this edition, we take a look at the recent payment aggregator guidelines issued by the regulator, which impact the card-on-file functionality. We will focus on the following areas:

- storage of cards by payment aggregators and merchants
- recurring payments.

We have analysed the key challenges faced by participants and the way forward in terms of alternatives for card-on-file transactions.

In addition to our views, we have presented our recommendations on key areas we feel should be looked into by participants, to minimise the impact of these guidelines.

I hope you find this newsletter to be a good and insightful read.

For further details or feedback, please write to:

vivek.belgavi@pwc.com or mihir.gandhi@pwc.com

Contents

01 Introduction to card on file

Over the last couple of years, India has seen tremendous growth in online retail, apparel, travel, over-the-top (OTT) media, food delivery, online medicine and e-consultation services. Growth in these areas has in turn helped online payment to grow significantly in India. While multiple payment options are offered by these merchants to customers, cards are one of the preferred modes. Merchants and their payment processors are trying to achieve convenient payment experiences by offering faster checkouts and one-click payment to customers. Card on file is one of the features which help achieve these objectives.

What is card on file?

A card on file, or stored credentials, is the card information stored by a merchant, payment gateway, payment aggregator or digital wallet to process future transactions.

These players store the card number and other relevant details related to a card in an encrypted format; however, the card verification value (CVV) is not stored. At the time of a card transaction, customer consent is taken to store these card details for future reference.

Typically, two stages are involved in the card-on-file functionality:

First stage: This is the first transaction for which the cardholder enters details to authorise the transaction with two-factor authentication (2FA) on any online platform. At the time of this transaction, the merchant typically asks for customer consent to store the details.

Second stage: This stage typically involves two scenarios:

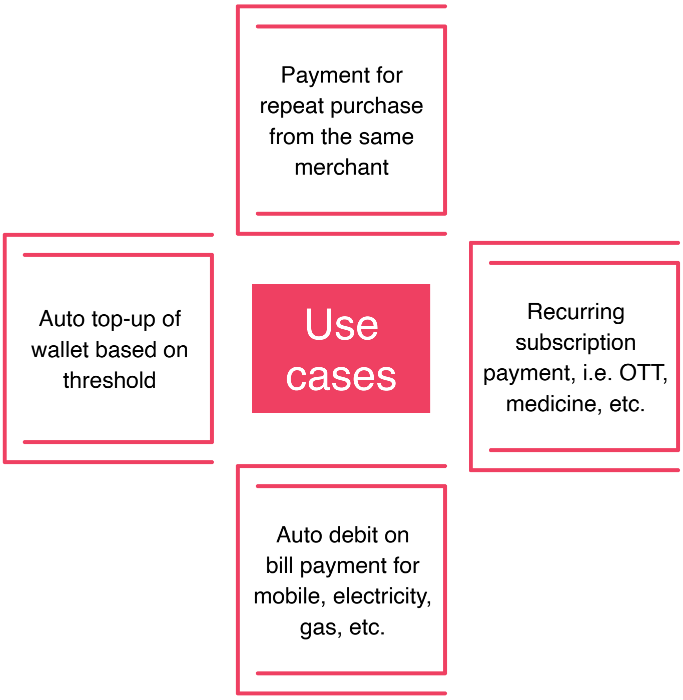
- The customer uses the stored card details on the merchant site and initiates a subsequent transaction with 2FA.
- The merchant uses the stored card details to initiate another transaction on the same website as the customer has provided consent for recurring transactions at the first stage.

What is the need for card on file?

Card on file is a very important feature in terms of customer convenience and making the transaction process smooth.
It has two main benefits:

- eliminates the need of re-entering card details on the merchant site
- helps in executing recurring payments.

Use cases for card on file


Payment for repeat purchase from the same merchant
Auto top-up of wallet based on threshold
Use cases
Recurring subscription payment, i.e. OTT, medicine, etc.
Auto debit on bill payment for mobile, electricity, gas, etc.

02

RBI guidelines and impact

Recent RBI guidelines

In 2019 and 2020, RBI issued two guidelines with respect to the security aspects of card on file and storage of card details by merchants or payment aggregators.

The following guidelines pertain to the card-on-file functionality:

Storage of card details

RBI issued a guideline on 17 March 2020 (updated on 17 November 2020) on 'Regulation of Payment Aggregators and Payment Gateways'.[1] According to the guideline, payment aggregators and merchants cannot store any sensitive customer information like card details and have to comply with the storage requirements applicable to payment system operators (PSOs). This guideline has to be implemented by payment aggregators and merchants by 31 December 2021.

Consent of the customer before executing recurring transactions/auto debit

In August 2019, RBI issued a guideline[2] for cards and PPI which was subsequently extended to UPI in January 2020. As per this guideline, 'Banks [have] to send a notification to customers five days prior to the payment being deducted and allow the transaction to go through only after the customer approves it.' This is applicable to recurring transactions on cards, UPI and digital wallets. Although the initial deadline to implement this on guideline was 31 March 2021, RBI has extended the same on 30 September 2021 in its latest circular issued on 31 March 2021.

Trigger for these guidelines

Online card transactions involve multiple entities such as merchants, payment gateways and financial institutions – each of which is as a potential risk entity for cyber criminals. Phishing, malware attacks, data theft are some of the categories of fraud related to card transactions and data.

- There has been an unprecedented spike in cases of data theft in the industry. According to the RBI's 2019–20 annual report, the number of registered frauds (cards and net banking) is increasing at a CAGR of 14%, while the value of frauds has increased at a CAGR of 34% in the last three years.
- Merchants/payment aggregator systems are being targeted to steal customers' sensitive financial and personal information.
- This information is leaked and sold on the dark web, causing economic as well as reputational damage for the payment service provider.

Data breaches have also seen a significant increase. Some recent incidents of data breaches that have made headlines are:

An Indian start-up was the victim of a massive data breach in 2020 which caused a large number of customer records to be out up for sale on the dark web. The company detected the breach immediately and acted quickly to stop the attack which could have resulted into leakage of more customer data.

A leading online grocery store faced a data breach in October 2020 which also led to the release of many customer records.

Sensitive debit card information was exposed to malware which caused a major security threat for an Indian payments service provide.

An East Asia based based cyber security company had over a million debit and credit card records stolen in 2019 including overseas customer data.

In 2021, the data of millions of digital wallet users was allegedly leaked onto the dark web despite the company denying any security breach.

[1] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0
[2] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11668&Mode=0

Challenges of AFA in recurring payments

01

The customer has to provide consent before auto debit is executed. This will dissolve the whole purpose of auto debit and the customer might miss the notification for consent which may lead to default or inconvenience.

02

Merchants, banks, card networks and payment aggregators have to make required technical and process changes at their end which will be cumbersome and costly.

03

Monthly transactions worth INR 2,000 crore will be impacted if participants are unable to comply with the guidelines on time.

Challenges of card storage guidelines

01

Customer payment experience could take a hit as customers would be required to enter the card details each time they make a purchase through the website.

02

Customers would use alternative payment modes (other than cards).

03

Recurring payments in case of subscription-based services would be impacted as the renewal cost would not be automatically deducted and the customer would be asked for the subscription/renewal fee for every cycle.

Impact of these guidelines on participants

The following participants will be impacted by these guidelines:

- merchants
- payment aggregators, payment gateways
- banks
- non-banks (NBFCs, wallet players etc.)
- card schemes.

The following are the major impacts:

Technological changes: All the participants have to make technical changes to their existing storage as well as recurring payment functionalities. Since these are standard and traditional functionalities provided by these players, it is a major change in terms of architecture and process.

Impact on subscription business: These guidelines will have a major impact on payment collection for subscription-based services like e-commerce, OTT media, e-pharma and food delivery. These companies have provided a seamless payment experience with the help of card on file. The RBI guidelines will hamper their payment collection process and may lead to a high customer churn rate.

Merchant dependency on acquiring banks: Some merchants store card details in an encrypted format. This helps them with the customer service, resolution of customer complaints, refund processing, etc. With these guidelines, merchants will have to rely on acquiring banks to address these concerns.

Monetary impact: Implementation of these guidelines will impose a cost burden on these players. Changes in tech architecture change, process changes, notification and consent from customers for recurring transactions and customer acquisition strategy changes will have an impact on their purses.

03 Way forward for participants

With the introduction of the new guidelines, the industry, as a whole, needs to look towards alternative solutions to provide customers with recurring payment solutions.

Tokenisation is an evolution of the current process that enhances transaction security. Tokenisation increases data security through encryption. Sensitive customer card information is replaced by a mathematically irreversible encrypted 'token' that is associated with the card number or with a previously authorised transaction. This token can be used for future transactions as well as recurring payments, eliminating the need for merchants to store any sensitive customer information.

Apart from tokenisation, changes in the card-on-file regulations can be addressed through alternative payment methods like UPI Autopay, e-NACH (National Automated Clearing House) mandates and digital wallets. While these solutions may not be able to replicate the process or experience of card-of-file transactions, they have their own advantages.

Tokenisation

Tokenisation is not a new concept and has been used as a security feature for card-saving and recurring payment services. Tokens are automatically generated in real time at the time of payment and do not slow down the payment process while preventing card information from hitting merchant servers.

Benefits

Tokenisation is the most logical solution for tackling the new card-on-file regulations. As tokenisation does not slow down the payment process, it would go unnoticed by the end user while eliminating the actual exchange of customer information.

While eliminating the exchange of card information, tokenisation does not eliminate the key advantages of card of file like easy recurring payments and quick checkouts. As the created tokens are reusable, the merchants are able to charge the token multiple times for recurring payments without customer intervention.

Apart from eliminating the need for storing card information, tokenisation will help increase customer trust in digital transactions as well as issuer confidence in approving transactions due to the additional security layers and lower chances of data breaches. It also helps eliminate some of the main causes for transaction rejections, providing a smoother user experience and enhanced customer and issuer trust as the information does not get outdated, unlike card information stored on file.

Benefits of tokenisation

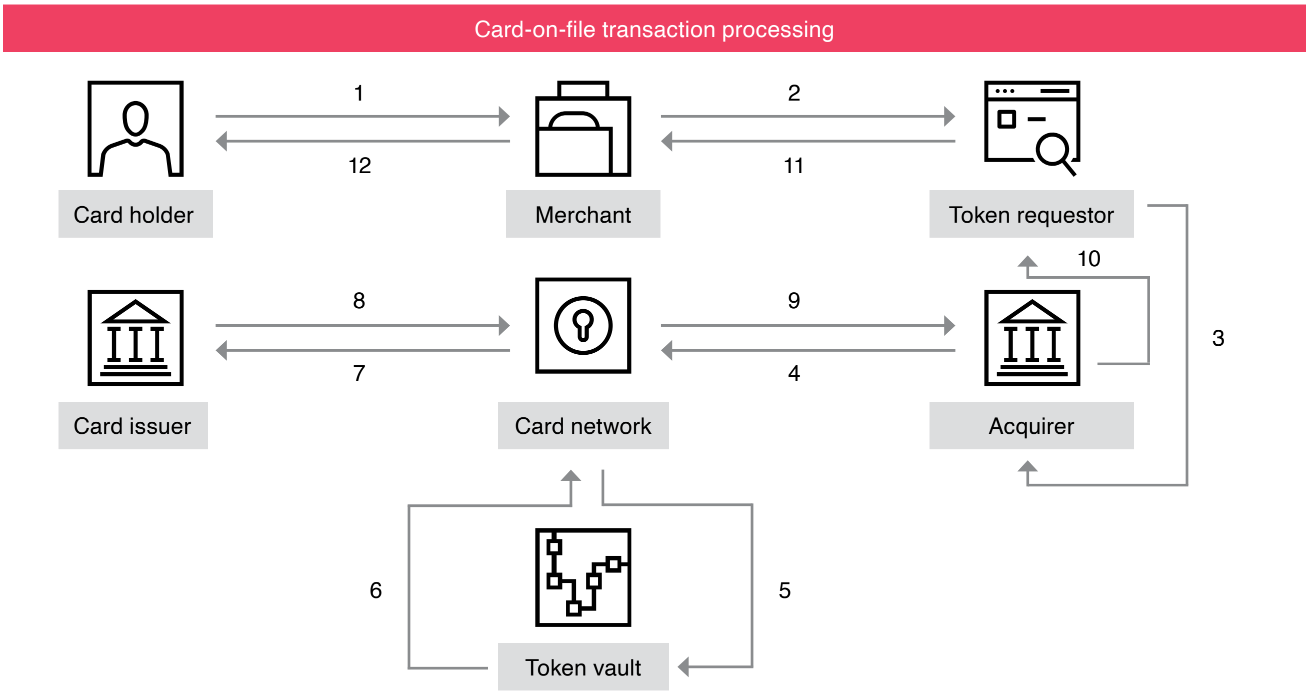
1 **Enhanced user experience**

2 **Increased data security**

3 **Increased customer and issuer trust**

4 **Reduced operating costs and liability expenses**

Process flow



When a transaction is initiated by the customer, the token requestor is responsible for sending the token information to the card network via the acquiring bank. The card network in turn communicates with the token vault to obtain the respective PAN and passes the same onto the card issuer. The card issuer is responsible for processing the request and executing any security protocols while relaying the transaction success or failure back to the network and the merchant. Despite there being additional steps in the payment process, these take place behind the scenes and do not impact the customer experience or transaction time significantly.

Challenges

Despite tokenisation being the seemingly obvious choice, implementation challenges would need to be considered and overcome to achieve widespread adoption. Changes will be required to incorporate tokenisation of card numbers which will increase the implementation time, but the benefits of offering tokenisation heavily outweigh the impact and costs.

There are a few additional challenges that need to be taken into consideration. Current regulations permit tokenisation of card credentials on mobiles/tablets only. With the growth of e-commerce assisted by the card-on-file functionality and emergence of new contactless payment modes, extending the guidelines to cover new uses cases like e-commerce, IoT and transit should be considered. Extending the guidelines on tokenisation to cover e-commerce as a use case will also partly reduce the challenges arising from the guidelines on recurring card transactions where card on file is a necessity.

Tokenisation will allow the closest replication of the functionality and usability of card-on-file transactions while also providing significantly more security for both users and merchants.

Alternative payment methods

Recent guidelines will have an impact on card transactions as customer convenience and recurring payments will be affected.

Customers will be tempted to consider other payment modes like UPI, NACH and digital wallets in place of cards. UPI has already eliminated some of the dependence on card transactions by allowing instant payment transactions over the IMPS infrastructure while offering services like proxy identifiers, low-limit recurring payments for subscriptions and low-value EMIs. Digital wallets have emerged as one of the major payment modes through new functionalities such as one-click payments, bill payments, auto debits and marketplace. e-NACH mandates have looked to address the high-value B2B and B2C recurring payment market, allowing customer to set limits and variable recurring payment amounts.

Despite the availability of these alternative methods and their advantages, it is difficult to consider them as replacements for card-on-file transactions. Although UPI has been considered a preferred mode for low-value retail transactions, RBI guidelines are applicable on recurring transactions through UPI. e-NACH mandates lack a seamless user experience with higher mandate initiation times. Also, like digital wallets, they involve additional steps or considerations which again limits their viability as true alternatives.

Comparative analysis between payment modes for recurring payments

Payment mode	Cards	UPI	e-NACH	Wallet
Factors				
Convenience	●	◕	◔	◑
Acceptance	●	●	◔	◑
Dispute resolution	●	◑	◔	◔
Security	●	●	●	◑

Source: PwC analysis

Conclusion

The changes in the RBI’s regulations will have a major impact on how customers choose to make payments and on how merchants ensure minimal disruption to the check-out experience. Tokenisation is the logical way forward with minimum impact on customers, but it requires major infrastructure changes by banks and merchants to accommodate the encryption process. There will be a learning curve and the industry as a whole will need time to adapt and adopt tokenisation.

Seamless completion of recurring transactions has been a significant factor for growth of digital transactions in bill payments, subscriptions, etc. While the need for instilling customer confidence cannot be overlooked, it should not be at the cost of their convenience. Ecosystem stakeholders will be required to develop solutions that can maintain a balance between customer data security and convenience on the one hand and satisfaction of RBI requirements and faster adoption by customers on the other.

Glossary	
IMPS	Immediate Payment Service
NACH	National Automated Clearing House
NBFC	Non-banking financial company
PAN	Permanent Account Number
PSO	Payment system operator
UPI	Unified Payments Interface

04

Payment technology updates

Debit card, credit card auto payment: RBI extended deadline for processing recurring transactions

Livemint

On 31 March, the Reserve Bank of India (RBI) extended the timeline for processing recurring online transactions by six months. Now banks and financial institutions have time until 30 September to implement the new framework.

Read more.

UPI transactions more than doubled in a year to 2.7 bn

Livemint

Transaction volumes over the Unified Payments Interface (UPI) more than doubled over a year, touching 2.73 billion in March 2021 compared to 1.25 billion a year ago.

Read more.

UPI volumes increase 77% year-on-year in Jan '21

Business Standard

UPI transaction volumes have increased to 2.3 billion (about 77%) compared to last year, and the value has doubled to INR 4.3 crore.

Read more.

Amazon plans to step up e-payments, financial services in India

Business Standard

Amazon India wish to convert cash-hardened customer into a digital one.

Read more.

Banks to decline auto pay transactions from April 1; here are the new rules on recurring payments

CNBC TV18

The regular automatic payments using debit and credit cards or prepaid payment instruments (PPIs) or UPI will be impacted from tomorrow.

Read more.

Will digital subscriptions see a slowdown after RBI's curb on storing card data?

INC 42

Recurring payments across streaming services, magazines and news portals are likely to be impacted after the RBI's new notification.

Read more.

Explained: The RBI's order on recurring payments on credit cards

Indian Express

Over the last few days, banks have started sending messages or emails to their credit card users intimating them that any standing instruction for recurring transactions will not be approved by the bank beginning 1 April 2021.

Read more.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Find out more about PwC India and tell us what matters to you by visiting us at www.pwc.in.

Contact us

Vivek Belgavi

Partner, Financial Services Technology Consulting, and India FinTech Leader

PwC India

vivek.belgavi@pwc.com

Mihir Gandhi

Partner and Leader, Payments Transformation

PwC India

Mobile: +91 99309 44573

mihir.gandhi@pwc.com

Contributors

Zubin Tafti
Aarushi Jain
Kanishk Sarkar
Tanmay Bhatt
Tushar Gupta

Data Classification: DC0 (Public)

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

PD/AW/May 2021-M&C 12238