KHAITAN & CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

RBI EXTENDING THE RESTRICTION ON STORAGE OF ACTUAL CARD DATA (CARD-ON-FILE) TO FACILITATE COMPLIANCE

1 July 2022

Introduction

At present, several participants, including merchants, are involved in the online card transaction chain, who store actual card (CoF) data like card number, expiry date, etc., citing cardholder convenience and ease of undertaking future transactions. While this practice is expedient for the end customers, availability of card details with multiple entities increases the risk of card data being stolen, misused, or compromised.

To safeguard consumer interests and protect privacy and security of customer data (especially any financial or personally identifiable information), the regulator has periodically revisited the compliance requirements and has imposed additional restrictions on all entities having access to customer data, from time to time.

Background

Since the payment aggregators (PAs) and payment gateways (PGs) perform important functions as intermediaries by facilitating online payments and handling of funds, the Reserve Bank of India (RBI) in continuation with the directions issued on 24 November 2009 for opening and operation of accounts and settlement of electronic payment transactions involving intermediaries, has on 17 March 2020, issued additional guidelines (read with the clarification dated 17 September 2020) regulating these intermediaries (Framework). Under this Framework neither the authorised payment aggregators, nor the merchants on-boarded by them, can store customer card credentials within their database or server.

On 31 March 2021, a 6 (six) months extension was provided for non-bank PAs until 31 December 2021, to enable the payment system providers and participants to establish workable solutions, such as tokenisation, within the Framework.

Initially tokenisation services were permitted only for devices which included mobile phones and tablets. Subsequently this facility was extended to laptops, desktops, wearables (e.g., wrist watches, bands, etc.), internet of things (IoT) devices, etc. On 7 September 2021, RBI issued a notification for tokenisation of card transactions, permitting card-on-file tokenisation (CoFT) services thereby extending the device-based tokenisation framework to CoFT as well and permitting the card issuers to offer card tokenisation services as token service providers (TSPs) only for the cards issued by or affiliated to them. The right to tokenise and de-tokenise the card data vests with the respective TSP and tokenisation of card data is to be undertaken with explicit customer consent requiring additional factor of authentication (AFA) validation by the card issuer.

Under this CoFT framework, cardholders can create "tokens" (as a unique alternate code) in lieu of card details. These tokens can then be stored by the merchants, for processing future transactions. Thus, CoFT is safer as it obviates the need to store or share card details with merchants while providing a similar degree of comfort to the cardholders.

Analysis

Consequently, with effect from 1 January 2022, no entity in the card transaction or payment chain (other than the card issuers and / or card networks), is permitted to store the actual card / CoF data, and any such data previously stored is required to be purged. For transaction tracking and / or reconciliation purposes, entities can store only limited data like last four digits of the actual card number and card issuer's name, in compliance with the applicable standards. The card networks are responsible for complete and ongoing compliance by all entities involved.

Subsequently, on 23 December 2021, this timeline was extended by 6 (six) months until June 30, 2022, to allow more time to the industry stakeholders for developing alternate mechanism(s) in addition to tokenisation to handle any use case (including recurring e-mandates, EMI option, etc.) or post-transaction activity (including chargeback handling, dispute resolution, reward / loyalty programme, etc.), that currently requires storage of CoF data by entities other than card issuers and card networks.

RBI after review and elaborate deliberation with all stakeholders, observed that while substantial advancement has been made in terms of token creation and processing of transactions based upon these tokens has also been initiated, tokenisation is yet to gain traction across all categories of merchants. Furthermore, since opting for CoFT (by creating tokens) is a voluntary exercise for the cardholders, those who do not wish to create a token can continue to transact as before by manually entering the card details at the time of undertaking the transaction (Guest Checkout Transaction) though this alternate system is yet to be implemented by all the industry stakeholders.

In view of the above, to avoid any disruption and inconvenience to the cardholders, RBI has on 24 June 2022 issued a notification under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007), further extending the timeline for tokenisation of debit and credit cards and storage of CoF data by another 3 (three) months, till 30 September 2022, after which such data is required to be purged.

Comments

Since many entities do not mandate AFA for authenticating card transactions, pilfered data in the hands of fraudsters may result in unauthorised transactions, embezzlement, misappropriation of funds and consequential monetary loss to cardholders. Hence, implementation of these regulatory compliances is imperative to preclude any data breach and security incidents.

With the prevalence of artificial intelligence enabled big data and enormous growth of online payment transactions, it is crucial for all stakeholders to implement a multi-pronged strategy including tokenisation and devising supplementary innovative means to ensure anonymisation and restricting storage of customer's actual card / CoF data.

This extended timeline is aimed at facilitating the readiness of all industry participants, for handling and processing of tokenised transactions, and employing additional novel measures for all post-transaction activities (including chargeback handling and settlement) related to Guest Checkout Transactions. Implementation of these processes adds an additional layer of security, thereby enhancing the cardholder's payment experience being delivered in a smooth and safe environment.

- *Achint Kaur (Counsel)*

For any queries please contact: editors@khaitanco.com

We have updated our Privacy Policy, which provides details of how we process your personal data and apply security measures. We will continue to communicate with you based on the information available with us. You may choose to unsubscribe from our communications at any time by clicking here.