Symbiosis Law School, Nagpur Multidisciplinary Law Review
Volume II Issue I (2022), ISSN: 2583-1984 (Online), Pg. Nos. 131-142

TOKENISATION AS A MEASURE TO SECURITISE THE PAYMENTS SPACE- A GUIDE TO IMPLEMENTATION

Heena Malhotra*

ABSTRACT

The RBI has proceeded to impose additional security measures in the digital payments space by introducing the tokenisation of card details. While the measure is taken to boost security and the public's faith in digital payments, there are certain limitations that might exist with respect to implementing such a feature. Tokenization is the process of replacing sensitive information, such as credit card numbers, with a unique identifier or token. This token can then be used for transactions without exposing sensitive information, reducing the risk of fraud and data breaches. To implement tokenization in the digital payments industry, it is necessary to adhere to applicable laws and regulations, which include data protection and privacy laws. This paper will analyse the legal and regulatory framework for tokenization and provide guidance on how to ensure compliance. Additionally, the paper will explore the potential challenges and limitations of tokenization and provide recommendations for addressing them. Overall, the paper will provide a comprehensive examination of the motivation, implementation, and legal considerations for tokenization in the digital payments sector in India.

Keywords: *Tokenisation; digital payments; security; compliance.*

* Student, Symbiosis Law School, Pune, Email: 18010125426@symlaw.ac.in.

TOKENISATION AS A MEASURE TO SECURITISE THE PAYMENTS SPACE- A GUIDE TO IMPLEMENTATION

Introduction: Understanding Tokens and Tokenisation

Tokenization replaces sensitive data with a unique set of characters (a.k.a. token) and keeps a table of tokens corresponding to the data they represent in a secure database.

Two types of tokens: HVTs and LVTs

HVTs or High-Value Tokens act as replacements for crucial payment information to complete a transaction but are not entirely devoid of extrinsic value. They can be linked to their history (recurrence/ frequency of use) and geography (it can flag anomalies in location). They can be exploited by someone other than the user.

LVTs, also known as Low-Value Tokens, have the role of substituting important payment data in payment transactions. However, their purpose differs from that of other payment methods. Unlike other methods, LVTs alone cannot fully execute a payment transaction. To function, an LVT must be matched to the essential payment information it represents, albeit in a tightly controlled fashion, as they can only work on one identified device and are **unique to 1 account**. This is done to detect the token being used apart from the rightful cardholder's authorised devices and geography. [1]

Banks should aim to develop **Low-Value Tokens (LVTs).** Although it will be a short-term irritant (as customers will have to enter a different token for different merchants and different devices), it will be a long-term boon for the security of digital transactions.

The RBI Circular: Card-on-File Tokenization

After repeated extensions of the deadline with respect to non-storage of Card-on-File by anyone other than card issuers and card networks and the purging of any such data previously stored, the final extension till 30th September 2022 was granted, post which all such data would be purged. This was done so as to afford the time stakeholders to devise alternate mechanisms

[1] Dawn M. Turner, *What is Banking-Grade Tokenization According to PCI DSS*, https://www.cryptomathic.com/news-events/blog/what-is-banking-grade-tokenization-according-to-pci-dss (last visited Jan 19, 2023).

with respect to such transaction processing. Such an extension was also granted to allow tokenization to gain traction as an alternative mechanism of transaction processing.

Certain legal security standards that are a sine qua non for this feature to be a success are as follows:

While the mandate of the circular is with respect to purging of Card-on-File data, tokenization has emerged and gain traction as an alternative method of transaction processing. Even though tokenization is not mandatory, it is an important feature for security purposes. Below-mentioned is the legal framework that encapsulates such a feature and is imperative for the success of the feature.

The laws including bye-laws, guidelines, industry standards, etc. surrounding tokenisation include

1. ***Guidelines on Regulation of Payment Aggregators ("PAs") and Payment Gateways*** ("PGs") (directive issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007))[2]:

- Restrictions on storage of card data for e-commerce merchants and PAs and PGs even if they have complied with the Payment Card Industry Data Security Standards. (Para no. 7.4)
- It called for relinquishing all card data of the end users by the merchants and non-bank Payment Aggregators. (Para 10.4)
- These guidelines are only applicable when the transaction is being made for deferred payments (i.e., advance payment for expected delivery in the near future).
- Exception: Transaction tracking by merchants: they can only store last 4 digits of the card number and the card issuer name for the purpose of tracking their transactions.
- The authorised card payment networks should be subject to security audits (minimum prescribed interval of a year) by empanelled auditors of the Indian Computer Emergency Response Team.[3] The reports will be submitted to the Department of Payment and Settlement Systems.

[2] Guidelines on Regulation of Payment Aggregators and Payment Gateways- Reserve Bank of India - Notifications, (2021), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12050&Mode=0 (last visited Jan 19, 2023).

[3] Adv. Tanmoy, *Indian Computer emergency response team*, ADVOCATE TANMOY LAW LIBRARY (2019), https://advocatetanmoy.com/2019/11/23/indian-computer-emergency-response-team/ (last visited Jan 19, 2023).

2. ***Payment Card Industry Data Security Standards (PCI-DSS)[4]:***

- It must be ensured that if a fraudster gains knowledge about multiple token-to-PAN ("Primary Account Number") pairs, it should not point towards a pattern that makes other PAN values predictable from knowledge of only tokens.
- The original PAN should not be computationally feasible from the knowledge of the token, a number of tokens, or a number of PAN/token pairs.
- It is crucial for the tokenization product must have a monitoring system in place that can detect malfunctions, anomalies, or suspicious behaviour that could indicate irregular token-to-PAN or PAN-to-token mapping requests or the presence of unauthorized activity during the tokenization process. Furthermore, the product must provide a means of alerting employees in case of such events and recording them for future reference. In addition to the monitoring system, the tokenization product must include a mechanism to differentiate between tokens and actual PANs. This mechanism can either be inherent in the product, such that resulting tokens have no format that could reasonably be interpreted as a PAN, or external, such as labels that are logically connected to the token.
- To maintain effective control over all access attempts and ensure consistent application of access control rules, all requests for mapping between tokens and PANs must be processed through a carefully evaluated application program interface (API).
- To verify the identity of the subject making the request, the authentication mechanism used should meet or exceed the standards specified in PCI DSS Requirement 8. This is necessary to ensure that the identity of the requester can be effectively authenticated, thereby reducing the risk of unauthorized access and misuse of the tokenization system.[5]

3. '***Card on File – Tokenization Services' ("2021 Circular")***[6]

- Obtaining explicit consent of the end users is mandatory. Those who do not opt for the tokenisation feature will have to enter their card details for each transaction. It shall be taken again in events of card renewal or replacement.

[4] Payment Card Industry Data Security Standard, https://www.pcisecuritystandards.org/document_library/ (last visited Jan 23, 2023).
[5] Tokenization Product Security Guidelines –Irreversible and Reversible Tokens, (2015), https://listings.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.
[6] Tokenisation of Card Transactions – Enhancements- Reserve Bank of India - Press Releases, (2021), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52188 (last visited Jan 19, 2023).

- Card issuers can offer card tokenization services as Token Service Providers (TSPs). TSP card issuers may only sign or deregister card data for cards issued by or associated with such card issuers.
- Additional Factor of Authentication (AFA) by the card issuer is the medium of obtaining customer consent for using this technology by individuals to make payment.
- The token has to be unique for a combination of card, Token Requestor, and merchant.
- De-registration should be afforded to the merchants and the non-bank mobile wallets. The Mobile wallets have to provide a list of merchants on which the tokens have been used by the cardholder and should have the option to deregister the token on a particular merchant.
- The PA must ensure that the merchant's infrastructure meets security standards such as PCI-DSS and PA-DSS, where applicable. [7]

4. Information Technology Act, 2000 [8]:

- Section 43A: Security Compliance: The sections list penalties for any entity that is negligent in implementing/maintaining reasonable security practices while p0ssessing, transacting or handling sensitive personal data or information in a computing resource while using, controlling, and it results in the loss was caused by negligence or unlawful gain for any person.[9]

- Section 72A: The law specifies penalties for the unauthorized disclosure of information in violation of a legally binding contract. If a person engages an intermediary who has access to any material containing personal information about another person as part of a lawful contract and then discloses that information without the individual's consent, they may face punishment that includes imprisonment of up to 3 years and/or a fine of Rs. 5 lakhs.[10]

[7] Renuka Sane et al., *Should Consumers Be Prohibited From Storing Card Data on the Internet?*, SSRN ELECTRONIC JOURNAL (2021), https://www.ssrn.com/abstract=3867979 (last visited Feb 6, 2022).
[8] The Information Technology Act, (No. Act 21 of 2000).
[9] Technology Law Analysis: presented by Nishith Desai Associates;, http://tmp.nishithdesai.com/old/New_Hotline/IT/Technology%20Law%20Analysis_June1811.htm (last visited Jan 23, 2023).
[10] R. K. Dewan & Co-Dr Mohan Dewan, *Personal Data Protection Laws in India*, LEXOLOGY (2020), https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d (last visited Jan 23, 2023).

- Section 79 sets out the conditions under which an intermediary is not liable for any third-party information or data communications link it hosts.

5. ***Storage of Payment System Data, 2018***[11]***:***

The Reserve Bank of India (RBI) has mandated that payment data related to transactions processed by Indian payment service providers or intermediaries must be stored on databases and servers located within India. This is to ensure that sensitive payment data is subject to the same level of data protection and security as other sensitive personal data.[12]

- In addition to the RBI's requirements, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 prescribe guidelines for the handling of sensitive personal data, including payment data. The rules require legitimate business entities to follow "reasonable security practices and procedures" based on the international standard IS/ISO/IEC 27001. Furthermore, the rules require an audit of security practices and procedures by an auditor at least once a year or when the legal entity significantly upgrades its computing resources and processes. These rules ensure that sensitive personal data, including payment data, is handled securely and per established standards.[13]

- By virtue of Rule 3, financial information such as bank account numbers, credit card details, debit card details, and other payment instrument details are classified as sensitive personal data**.**

- Rule 4 of the 2011 Rules requires that any entity (or person acting on behalf of the entity) that collects, receives, holds, stores, trades or handles information from information providers must provide a privacy policy. Such privacy policies should be available for inspection by those who have provided information to the legal entity under lawful contracts. The privacy statement must also be published on the company's website. The privacy policy should set out the company's practices and policies for the collection, receipt, possession, storage, trading or handling of information. It should

[11] Storage of Payment System Data; Reserve Bank of India - Press Releases, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244 (last visited Jan 23, 2023).
[12] Background on Indian government regulations affecting card payments : Stripe: Help & Support, https://support.stripe.com/questions/background-on-indian-government-regulations-affecting-card-payments (last visited Jan 23, 2023).
[13] Supra, note 3.

also list the type of personal information or sensitive personal information collected from the legal entity.

- Under sub-rule 7 of rule 5, it is required that the "information provider" be given the opportunity to withdraw any consent that was previously provided to a legal entity.

- Rule 8 of the 2011 Rules provides guidelines for appropriate security practices and procedures that must be followed by legal corporate entities or persons acting on their behalf. In order to demonstrate that appropriate security practices and procedures have been followed, the entity must have a comprehensive, documented information security program in place. This program must include security policies and controls that are appropriate for the business's nature and the protected information assets. These controls may include managerial, technical, operational, and physical security controls. Under Rule 8(2), the International Standard IS/ISO/IEC 27001 is considered to be an appropriate standard for information security management systems. This standard outlines requirements for establishing, implementing, maintaining, and continually improving an information security management system. Compliance with this standard can help ensure appropriate security practices and procedures are in place. The RBI has also issued guidelines that obligate banks to comply with the IS0/IEC 27001 and IS0/IEC 27002 standards. These guidelines are intended to ensure that banks have appropriate security measures in place to protect sensitive financial information and other personal data..

- The COBIT or Control Objectives for Information and Related Technology is another framework that is not precluded under these Rules. These can form a good internal framework for an organisation.

6. Reserve Bank of India: Notification, 2019: As per the RBI's guidelines, Additional Factor of Authentication (AFA) & PIN number Entry for every transaction is still a requisite.

Requisite regulatory compliances to be ensured before offering Tokenisation in an IoT Product

Amazon has already started experimenting with Amazon Go Points of Sale, with the first store opening in London in March 2021. In these stores, payments are made automatically, which

raises concerns about user recognition and tracing. While these payments are initiated autonomously, they are ultimately charged to a user's wallet or account. Therefore, the user is a natural person with a financial capacity. In this form of payment, requiring the user's biometric for identification would be a limitation, as suggested for the above problem.

Applicable Laws

The RBI has expanded the scope of devices that can utilize tokenization in its Circular titled Tokenisation – Card Transactions: Extending the Scope of Permitted Devices[14], to include devices such as laptops, desktops, wearable devices like watches and cassettes, and Internet of Things (IoT) devices. While Indian regulations have not kept pace with technological advancements, traditional regulations like the IT Act, 2000 Reasonable Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 can be implemented.

- Section 43A of the IT Act holds corporate bodies liable to pay compensation for damages caused by breach of confidentiality of Sensitive Personal Data of individuals due to their negligent acts.
- Additionally, Section 72 of the IT Act outlines the penalty for breach of confidentiality and privacy of collected data.[15]

Apart from the above, the following standards/guidelines will be applicable for the Tokenisation service for payments on IoT devices as per the RBI circular: [16]

- The e-commerce will have to relinquish all the personal card details of the users
- Merchants in India must obtain authorization from Indian cardholders and provide 24 hours' notice for any recurring payments or subscriptions exceeding Rs. 5000. This can be done through an e-mandate recorded by the issuing bank.
- The cardholder must also be given at least 24 hours' notice prior to the card issuer processing a charge.
- The cardholder must authorize each additional payment individually.

[14] Tokenisation – Card Transactions : Extending the Scope of Permitted Devices- Reserve Bank of India - Notifications, (2021), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12152&Mode=0 (last visited Jan 23, 2023).
[15] IIPRD, *Brief Note On SPDI*, IIPRD BLOG - INTELLECTUAL PROPERTY DISCUSSIONS (2020), https://iiprd.wordpress.com/2020/06/10/brief-note-on-spdi/ (last visited Jan 23, 2023).
[16] Processing of e-mandate on cards for recurring transactions- Reserve Bank of India - Notifications, (2019), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11668 (last visited Jan 23, 2023).

- Cardholders must be allowed the option to easily revoke and stop making recurring payments to a business through their bank at any time.

The modifications were implemented to provide more authority to cardholders but have also caused substantial hindrance to recurring payment procedures, which could lead to an increase in recurring payments being turned down by issuing banks.[17]

The Bank has recently implemented specific policies to promote card payments and ensure that card transactions meet the necessary security requirements to instil confidence in its users. These policies cover both face-to-face transactions (such as proximity payments) and remote transactions (such as online payments). Some of the measures taken by the Bank include:

- To promote card payments and ensure user security, the Bank has implemented specific policies for all CP and CNP transactions. As part of these measures, cardholders should receive online alerts for all card transactions, including both CP and CNP transactions, regardless of the transaction value. These alerts are designed to notify customers of transactions made with their card(s), including any fraudulent transactions so that customers can take immediate action to prevent or correct any issues;
- To provide an extra layer of security for all card non-present (CNP) transactions, an additional verification factor (AFA) must be implemented. This verification process requires the customer to provide information that only they should know to complete the transaction;
- For all card transactions with debit cards, a point-of-sale PIN is required to prevent the use of cloned cards and ensure that only the customer knows the PIN.
- Thresholds are set for international transactions made with existing magnetic stripe cards enabled for international use to minimize losses in case of fraudulent use of such cards.
- Migration of all cards to EMV chip and PIN to reduce fraudulent use of cloned cards and increase security in CP transactions.
- The card data can only be signed or rejected by the TSPs who have sole authority.

Other than the above-mentioned regulations, the IoT service provider may have specific privacy policies covering the scope and extent of use of the sensitive private information collected by the service provider and the measures taken to protect the information collected.[18]

[17] Framework for processing of e-mandates for recurring online transactions- Reserve Bank of India - Notifications, (2021), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12051 (last visited Jan 23, 2023).
[18] Supra, note 11.

Internal Frameworks that must be ensured

Banks can implement the following Internal Framework. The COBIT (or the Control Objectives for IT) is a complete management and governance framework with the following key features:

- Holistic approach.
- Ability to adapt to encounter the specific needs of stakeholders involved.

The COBIT lays down guidelines that can guide an organisation's internal policies based on specific goals. Its five principles and seven enablers can build an ample framework, serving organizations to attain their objectives.

Necessary contractual safeguards to be ensured by Banks

- It should be agreed between the Bank and the Token Requestor that the Personal data of the end users shall not be made available publicly under any circumstances.
- The RBI Directive of 2019 allows banks to include a clause in their agreements with merchants to check the security of the merchant's systems, applications, and features. This includes ensuring authorized access to the application on the device, as well as other processes such as customer onboarding, token provisioning and storage, data storage, and transaction processing. The checks must be carried out periodically, in accordance with Annexure 1 of the RBI Directive.
- The licensee should be liable to provide all information that the licensor demands to verify that the licensee is complying with the provisions of the agreement.
- The licensee should limit its liability from a security breach occurring out of acts attributable to the systems of merchants that leaks customer data or causes any loss to the end user.
- The licensee should limit its liability from a security breach occurring out of acts attributable to the end user whether or not it has authorised the transaction unless the card details have been removed from the mobile wallets or e-commerce platforms.
- If there is any anomaly or suspicion on the performance of an end user's card, the bank should have the right to suspend/terminate the validity of the card and order removal of the card details from merchant platforms.
- A provision for the compromise of security/possession of the end user's card or device or the security details of the card or the device should be reported to the Bank.

- There should be an express mention of the extent of liability in case of fraud attributable to Banks or the merchant application.

Market Scoping for additional security over Tokenization technology

Apple Pay had introduced a double token technology (in simple terms), accessible with a biometric layer of security like fingerprint or face recognition. So when the consumer wants to use the enrolled card at a terminal that supports Apple Pay they first need to biometrically authenticate on the phone. Then the token stored on the phone acts like a credit card number and is used like EMV with the terminal to generate yet another random number.

Apple Pay is often compared with mobile wallet services like Alipay or WeChat Pay which were launched roughly around the same time. Both were highly hyped to dominate the mobile payment space in their respective markets. However, as the mobile wallets achieved nearly ubiquitous adoption very quickly in the Chinese market, Apple Pay still needed to achieve the same market share in the US and the overall adoption rate was quite low particularly, in its early years.

The author feels that Apple and Google for that matter are not really getting the right message across. After reviewing their technology, the key distinguishing feature of the services is more security. However**,** the consumers usually need to learn about that. Their marketing strategy on the launch of the product was convenience rather than focusing on security. Many consumers are still unaware of the major threats to their savings through online transactions. Neither technology nor the law has been even decently successful in tracking down fraudsters.

Hence, the major marketing focus of IRC Bank in communicating to its consumers must be the additional security that is afforded through the tokenisation technology or any other feature on it.

Conclusion

The author would like to suggest that there should be an obligation to disclose to the public of any breach or leak of their payment details. There is currently no obligation to report cyber incidents (threats or breaches) to the public. However, according to the Intermediary Guidelines, intermediaries must notify CERT-In of cyber security breaches as soon as possible.

A general opinion of the author is that while this move is a commendable move towards more secure payment solutions, the RBI should not have precluded the other mechanisms that were

in place. If the existing security mechanisms were insufficient, the RBI should have provided data on the frauds attributable to the existing security standards and tokenisation could have been an optional move for the consumers. This is also an anti-competitive approach which precludes players that offer conventional security without much concrete reasons.