The Dialogue™
INFORM ENGAGE IDEATE

DEEPSTRAT
STRATEGY. POLICY. ACTION

COF AND TOKENISATION GUIDELINES

ANALYSING THE POTENTIAL IMPACT ON DIGITAL PAYMENTS INDUSTRY

RBI's CoF and Tokenisation Guidelines - Analysing the Potential Impact on Digital Payments Industry

ACKNOWLEDGEMENT

The research team would like to express our gratitude to Saikat Datta, Strategic Advisor, The Dialogue and Founding Partner, DeepStrat, for his guidance, encouragement, and useful critique of this report. The team would also like to extend our sincere thanks to the participants of our stakeholder interviews for offering us their time and resources in collecting inputs for the report. We are further grateful to Subhasmita Priyadarsani and Bhavya Birla for providing research assistance on this report.

We also express our sincere thanks to Kazim Rizvi, Founding Director of the Dialogue for his guidance and inputs on multiple drafts of this report.

Authors' Note: A submission was shared with the RBI before the announcement of the deadline extension for deleting card on file details. This report is an extended and a more detailed version of that submission. We are thankful to the RBI for their receptiveness to industry feedback and commitment towards building enabling frameworks for the payments industry. In addition to suggesting a six-month extension of the deadline, the report also recommends other steps for the industry and the RBI on the basis of stakeholder inputs and secondary research. We believe that these insights play an important role in guiding the public discourse. This report is being made publicly available to inform and nurture more discussions around the tokenisation mandate.

ABOUT THE AUTHORS

Anand Venkatnarayanan - Strategic Advisor, DeepStrat

Ayush Tripathi - Senior Research Associate, The Dialogue

Gautam Kathuria - Senior Research Associate, The Dialogue

Saksham Malik - Senior Research Associate, The Dialogue

*These names have been arranged alphabetically

METHODOLOGY

The Dialogue and DeepStrat conducted a series of interviews with key stakeholders in the digital payments ecosystem which are impacted by these regulations. These interviews helped garner insights from members of the digital payments community in terms of their sentiments on the RBI's CoF and tokenisation framework.

This report is an effort to understand the impact of these guidelines on the payments ecosystem in India. It has analysis conducted by the team at The Dialogue and DeepStrat by combining inputs collected by the stakeholders with existing literature that was reviewed throughout the process.

TABLE OF CONTENTS

KEY RECOMMENDATIONS

1. Extending the Deadline

- Defer the implementation of the clause necessitating deletion of card details by at least six months to carry out audits of banks and check their preparedness to ensure that transition to tokenisation is smooth.

2. Phased Implementation and Auditing

- A phased implementation approach should be taken for Card on File Tokenisation (CoFT) with a focus on achieving key milestones such as tokenisation of new cards, completely migrating the existing users to new schemes, checking downstream impact, etc.
- Ensure audits of the stakeholders regulated by RBI for minimal disruption. The audits of tokenisation system of banks, card networks and other token service providers is crucial. These audits should evaluate the preparedness in terms of various factors, including internal processes and technical infrastructure to carry out tokenisation.

3. Analysing security standards for stakeholders

- From a cybersecurity standpoint, tokenisation could lead to creating issues around data integrity. Any cybersecurity structure banks on the three principles of Confidentiality, Integrity and Accessibility. Therefore, this aspect must be factored in before implementing tokenisation.
- Set uniform and enhanced security standards for all stakeholders storing card details under the tokenisation framework. These stakeholders could be any one in the transaction chain including banks, card networks, merchants etc.
- Analyse the security aspects of vault tokenisation and come up with a whitepaper discussing the cybersecurity concerns and complexities arising out of creating repositories of data.

4. Adopting a consultative approach for future regulations

- For future regulations, RBI may consider adopting an open stakeholder consultative process to ensure transparency. Another factor that would help the RBI become more transparent is to publish stakeholders' responses, either anonymised or public as RBI deems fit. This would ensure accountability and provide transparency in terms of suggestions made to the regulator.

I. INTRODUCTION

The digital payments industry has been one of the pillars of India's rapidly growing digital economy. It is expected to grow at a compound annual growth rate (CAGR) of 27% during the FY 20-25 period, with reports projecting the rise in digital payment transactions from Rs 2,153 lakh crore in FY20 to Rs 7,092 lakh crore in FY25[1]**.** The payments ecosystem in India comprises a variety of stakeholders - from payment gateways and aggregators, to banks, wallet providers, as well as merchant sites themselves. The technological developments have led to a greater degree of streamlined coordination between these financial institutions.

This stellar growth is being actively driven by the exponential rise in supply and demand side dynamics. On the demand side, a rapidly growing consumer base, driven by increasing smartphone penetration and availability of the internet has brought about a paradigm shift in digital financial inclusion. Digital modes of payment, though still lagging behind cash payments, have emerged as strong competitors. The supply side dynamics are built on a foundation of fierce competition, technological innovation, and an overall focus on consumer convenience in integrating digital financial services in their everyday lives.

Onboarding of several small businesses has given further impetus to the growth of digital payments, with payment service providers providing incentives for businesses, including automated account keeping services, and the requisite hardware and software integration. Policy frameworks promoting adoption and penetration of digital payments and a conducive environment for cashless payments, necessitated by Covid-19, has accelerated the development of this sector. There is also a greater thrust on the role of digital payments in integrating online and offline markets. **The RBI has taken a proactive role in providing a regulatory foundation for this growth, and is now attempting to strike a balance between consumer convenience and security of financial data.**

[1] Soni,S. (2021 March 21) *'Digital Payments to Skyrocket 3X to over Rs 7,000 Lakh Cr by FY25; Mobile Payments to See Highest Growth.'*,Financial Express, Retrieved from https://www.financialexpress.com/industry/banking-finance/digital-payments-to-skyrocket-3x-to-over-rs-7000-lakh-cr-by-fy25-mobile-payments-to-see-highest-growth/2217233/.

II. BACKGROUND ON RECENT PAYMENT REGULATIONS

The most notable attempt in this direction was the Guidelines on Regulation of Payment Aggregators and Payment Gateways (PAPG Guidelines)[2]. These regulations aimed to regulate PAs and PGs in their entirety, apart from aspects of baseline technology standards and account management. Among other measures, it mandated that merchant sites, payment aggregators (PAs) and payment gateways (PGs) would not store sensitive customer information such as card details. The guidelines regarding e-mandates also underwent changes, now requiring banks to send pre-debit notification and mandate management to customers, without which customers need to enter card details and payment approval during every recurring transaction.

More recently, the RBI introduced rules that disallowed storage of Card on File (CoF) by merchants and aggregators. However, card issuers were allowed to store details. A CoF or stored credentials, is the card information stored by a merchant, PG, PA or digital wallet to process future transactions. These rules may also be supplemented with proposed guidelines for CoFT[3], which is the only RBI-approved alternative to storing CoF, and seeks to balance the convenience of storing necessary financial data of customers on the merchant platform, while ensuring the need for the safety and security of such data. Reducing the retention of CoF data has also been seen as an instrument to control the sharing of sensitive customer data with third parties and giving customers more autonomy in the sharing of such data.

III. CoF AND TOKENISATION

1. Card on File

A CoF or stored credentials, is the card information stored by a merchant, PG, PA or digital wallet to process future transactions. The storage of card credentials on the merchants' platform makes transactions much easier, as customers do not have to enter card details during every such transaction. It also allows for processing refunds, grants of promotions or offers, making recurring payments, converting payments into EMIs etc.

[2] RBI Notifications (2020, November 17), '*Guidelines on Regulation of Payment Aggregators and Payment Gateways,* Reserve Bank of India *(Updated as on November 17, 2020)'* Retrieved from https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11822&Mode=0

[3] RBI Press Release. (2021, September 7), *'Tokenization of Card Transactions – Enhancements',* Reserve Bank of India, Retrieved from (https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52188)

2. Benefits of CoF

CoF storage provides a frictionless means of payment for goods and services provided, due to the readily available nature of the card information on the consumer's account. This facilitates seamless payments to be performed by customers who may not be as digitally savvy, with a one time storage of card credentials simplifying their future transactions as well.
On the supply side, CoF enables easier provision of goods and services paid for digitally, including one-time and subscription based services, due to smooth processing owing to low friction , in addition to less intrusive prompts by the merchant. It also allows for multiple use cases like grants of offers, reconciling refunds, converting high ticket transactions into EMIs, etc. The flexibility offered in terms of storing, modifying, or deleting card credentials is another advantage, which balances consumer autonomy with ease of transactions. The lawful sharing of customer data also allows for more accurate digital advertising of products and services, which may in turn raise the possibility of a higher number of digital transactions, and growth of smaller online-only businesses.

3. Tokenisation

The move towards limiting CoF storage potentially risks business continuity and ease of payments on both sides - businesses and customers. Expanding the ambit of tokenisation is a countermeasure, with the RBI suggesting payment service providers to implement tokenisation of CoF data. Tokenisation of this data enhances the level of security (in addition to the necessity of PCI-DSS compliance of merchants and payment service providers), while causing reduced disruption in billing cycles. The RBI's directives to introduce tokenisation of card details is another step towards improving overall transaction safety. The recent regulations are an extension of the earlier regulation pertaining to the device-based tokenisation framework advised vide circulars of January 2019 and August 2021 to CoFT as well. Thus, card issuers may now offer tokenisation services as well, with explicit customer consent needed for implementation.

Card tokenisation is a process where sensitive customer data (such as card number, CVV, etc.) is replaced by an algorithmically generated token (encrypted), provided by the token service provider. Currently, banks and card networks have been permitted to act as token service providers.. These tokens flow through payment systems in a secure manner[4], without disclosing the customer details or allowing the payment intermediaries (e.g. merchants, PAs) to store

[4] Rastogi R. , The Paypers (2021, November 25) *'RBI's Card on File Storage Restriction Rules- Is Tokenization the Answer?'* The Payers, Retrieved from https://thepaypers.com/interviews/rbis-card-on-file-storage-restrictions-rules-is-tokenization-the-answer--1253039

customer data. Tokenisation works after a request for the same has been made by the cardholder on the app provided by the token requestor. Then, coordination mechanisms between the token requestor and the card issuer ensure that a unique token is issued after a request has been made. This token is based on a unique combination that corresponds to the card itself, the token requestor, and the Email ID/Phone number used by the token requestor. In network tokenisation, the token gets linked to a customer's email/ phone number, and generates a unique token for each merchant-card linkage. For subsequent transactions, the token request mechanisms ensure that only the tokens corresponding to a card are shared, and not the real customer data.

The CoF tokenisation provides significant expected benefits, enhancing security of financial data, while retaining consumer convenience.

4. RBI's View

The digital payments sector has been among the fastest growing sectors within the financial services domain, with nearly 31% growth in FY 2020-21[5], and an expected coverage of nearly 70% of all payments by 2025[6]. With respect to share of digital transactions, credit and debit cards have been witnessing a good growth trajectory. High competition, built on a foundation of customer acquisition, innovation, and ease of transactions, has characterised this sector. This has also enabled the digital and financial inclusion of scores of people, which would have been difficult without the thrust on digital payments.

However, this growth must also be seen in the context of the threat it presents- not just in terms of the technological risks, but also the greater degree of vulnerability faced by less digitally savvy populations. Frauds may be categorised[7] into buyer side frauds, merchant side frauds, and cybersecurity related frauds, with COVID-19 also creating a hospitable environment for such incidents to increase. Reports point out that nearly half of the bank frauds in India are digital

[5] PTI (2021, July 28) *'Digital Payments up 30.2% in FY21: RBI Data,'*, The Economic Times, Retrieved from https://economictimes.indiatimes.com/news/economy/finance/digital-payments-up-30-2-in-fy21-rbi-data/articleshow/84828643.cms

[6] Awasthi, R. (2021, March 31), *'Digital Payments in India to grow to 71.7% of all payment transactions by 2025: Report'* The Hindu, Retrieved from https://www.thehindubusinessline.com/news/digital-payments-in-india-to-grow-to-717-of-all-payment-transactions-by-2025-report/article34204827.ece

[7] DSCI, and Paypal.(2020), *'Fraud & Risk Management in Digital Payments'* Data Security Council of India, Retrieved from https://www.dsci.in/sites/default/files/documents/resource_centre/Fraud%20%26%20Risk%20Management%20in%20Digital%20Payments.pdf

payment frauds[8], a trend that can be observed in the value of frauds increasing at a CAGR of 34% over the last three years[9]. These numbers may be better understood from the National Crime Record Bureau's observations[10], which state that cases of online financial fraud using credit or debit cards have seen an increase of over 225 % amid the pandemic - from 367 in 2019 to 1194 in 2020. The value of these frauds over a decade is also a concern, with the RBI reporting[11] a loss of nearly Rs.615 crore over the last 10 years. Further, there is a possibility of this amount being much greater as it does not include cases of fraud below Rs 1 lakh.

Another technological vulnerability arises from the risk of breach of sensitive customer data, and its unauthorised sharing or sale. The last few years have witnessed massive data breaches at large private companies including Hitachi, Mobikwik, Juspay, Big Basket, and BHIM UPI, with the efficacy of these companies' data security practices coming into question. Further, a significant proportion of citizens are feeling increasingly vulnerable to scams in the pandemic era.[12] Therefore, a case for regulations pertaining to enhanced security of consumer data can be made.

The RBI's concerns also emanate from the view that sharing card details across multiple merchant portals reduces consumer control over the security of their card data, and any attack on one merchant portal would translate to an overarching compromise of an individual's financial data. The emphasis on protection of customer data from leakages is reflected in the RBI's press release of September 2021, where it mentions that "Any leakage of CoF data can have serious repercussions because many jurisdictions do not require an AFA [Additional Factor Authentication] for card transactions." The same report also mentions that "The tokenisation of card data shall be done with explicit customer consent requiring Additional Factor of Authentication (AFA)."

---

[8] Gupta, S. (2020, January 30), *'Cybersecurity a critical challenge for india's digital payments ecosystem'*, Livemint, Retrieved from https://www.livemint.com/opinion/online-views/opinion-cybersecurity-a-critical-challenge-for-india-s-digital-payments-ecosys-11580402045918.html

[9] PwC India, (2021) *'Impact of RBI Guidelines on card Payment Transactions'*, PricewaterhouseCoopers, Retrieved from https://www.pwc.in/consulting/financial-services/fintech/dp/impact-of-rbi-guidelines-on-card-on-file-transactions.html

[10] *Crime in India 2020*. National Crime Records Bureau.

[11] Naidu,J.S. (2020, February 11) *'₹615.39cr lost to debit, credit card frauds'*, Hindustan Times, Retrieved from https://www.hindustantimes.com/mumbai-news/615-39cr-lost-to-debit-credit-card-frauds/story-E335UM0fj1dVKJYZcJ2zRN.html

[12] Indo-Asian News Service. (2021, June 10), *'Concerns over digital payments fraud grows in India: Survey'*, The Economic Times, Retrieved from https://cio.economictimes.indiatimes.com/news/internet/concerns-over-digital-payments-fraud-grows-in-india-survey/83390853

Further, while the RBI has a responsibility to create a conducive environment for the segment of society that have integrated well into the digital financial system, it also has a responsibility to protect those populations who have not. It is in this context that the above regulations have been formulated, keeping in mind the importance of both- consumer protection and safety, and seamless business continuity. A balanced regulatory regime thus offers both incentives- one for consumers to shift towards digital payments and digital financial inclusion, and another for businesses, to focus on greater penetration and ease of provision of financial services.

IV. CHALLENGES TO REMOVING COF AND IMPLEMENTATION OF TOKENISATION

The key recommendations of the paper; i.e., extending the deadline, phased implementation and auditing, adopting a consultative approach for future regulations and analysing security standards for stakeholders have been designed keeping the potential impact of removing CoF and implementing tokenisation. These aspects have been detailed below.

Over the years, the storage of card details has presented various benefits for different stakeholders in the payment ecosystem. The continued usage of this tool is crucial to extract long-term benefits for merchants, PAs/PGs, banks and consumers. But implementing a new system and prohibiting storage of card details may, therefore, invite several difficulties.

Following are some of the considerations and challenges that need to be kept in mind:

1. Challenges pertaining to removing CoF

a. Impact on customer convenience and inclusion

Convenience or ease of use is valued by consumers and is an important determinant for adoption of digital payment technologies.[13] A recent survey revealed that at least 82% consumers consider it would be somewhat or extremely inconvenient for them to re-enter all their card details for every card-based online payment.[14] Indians are significantly reliant on card payments for online purchases. In 2019, cards were the most commonly used method to pay online, accounting for 31% of all transactions. While it is forecasted that by 2023, digital wallets will overtake card

[13] Shree,S. (2021, January 5), *'Digital payments and consumer experience in India: a survey based empirical study'*, Springer, Retrieved from https://link.springer.com/article/10.1007/s42786-020-00024-z.
[14] Alawadhi,N. (2021 December 20), *Most consumers wary of stricter rules for online card use: Survey,* Business Standard, Retrieved from: https://www.business-standard.com/article/economy-policy/most-consumers-wary-of-stricter-rules-for-online-card-use-survey-121122001024_1.html

payments, the latter will still account for a significant share of 32% of all transactions.[15] It has been observed that customers often use services of the same merchant on multiple occasions. Therefore, the facility of not having to insert card details for each transaction is an important convenience. Being able to quickly pay without having to repeatedly enter details is an important consideration for making repeat purchases on e-commerce platforms. Therefore, if merchants are unable to store card details without any alternative mechanism, the customer experience can suffer significantly.

In addition to convenience, the ability to pay through stored financial details can also impact adoption of digital payment methods. For groups with limited digital financial literacy, including rural customers and the elderly, significant hand holding is required to partake in digital payment systems.[16] Customers often rely on family, friends as well as agents of financial institutions to adopt digital payments who help them set up a solution and save the required details. Amplifying the requirement to repeatedly enter details can add complexity to the process and require continuous hand-holding. The simplification and ease of use of digital payments is, therefore, necessary for digital and financial inclusion of certain groups.

b. Business implications for online merchants

A cumbersome experience for customers affects the business of online merchants. Businesses with an online presence, including private labels, strive to build long-term relationships with customers in order to ensure repeat purchases. In 2020, the share of online repeat purchases of private labels was more than 50%. An integral tool to ensure repeat business is by providing seamless payment mechanisms, including the ability to conveniently access payment details.[17] A significant volume of e-commerce transactions in the country is done through cards. In Q1 2021 itself, the number of e-commerce transactions through debit cards and credit cards were 458.31 million and 244.24 million respectively.[18]

Repeat transactions are especially important for businesses providing subscription based services, since these services involve regular weekly, monthly or yearly payments. If businesses are unable to provide regular customers a smooth card payment experience, they risk losing the

[15] JP Morgan (2021), *'2020 E-commerce Payments Trends Report: India'*, JP Morgan, Retrieved from https://www.jpmorgan.com/merchant-services/insights/reports/india-2020.
[16] mStar (2019, March), '*India Digital Financial Inclusion Journey Map Report',* USAID, Retrieved from https://www.usaid.gov/sites/default/files/documents/15396/mSTAR_IndiaDFI_Report_DRAFT_FINAL.pdf
[17] Statista Research Department (2021, July 29), *'Share of online repeat purchase of private labels in India 2020, by category',* Statista, Retrieved from https://www.statista.com/statistics/1227653/india-share-of-online-repeat-purchase-of-private-labels/
[18] Rongala,S. (2021), '*India Digital Payments Report',* Worldline, Retrieved from https://worldline.com/content/dam/worldline/documents/india/documents/worldline-india-digital-payments-report-q1-2021.pdf

customer which may lead to a loss of revenue. The loss can especially affect small merchants substantially. Further, companies utilize consumer data, including financial data to innovate and personalize their product and services. The inability to store data may hamper these capabilities. At the industry level, regulatory barriers for merchants to seamlessly process transactions has the potential to create an adverse impact on investor outlook on the ease of doing business in the country.

c. Issues pertaining to the transaction lifecycle

Transaction lifecycles do not merely involve payments from customers to merchants as consideration for services. The lifecycle also involves reconciliation of payments at the merchant's end. Notably, certain downstream transactions from the merchant to the consumer, including processing of refunds and cashbacks due to offers and promotions, may also form a part of it. Refunds to customers may be required in various scenarios, including but not limited to refund due to deficiency in services and transaction failure. Refunds are either added as credits to the customer's account with the online merchant or are reversed to the source used for making the payment.

In cases where customers use their cards for payments, refund of the amount to the source requires relevant debit or credit card details. In order to process the refund to the source, it is essential to store card information. In e-commerce, a good return policy[19], which includes quick processing of refunds[20], forms an integral part of the consumer experience. In the Indian context as well, research has indicated that time taken for settlements of wrong/excess payments and refunds for defective products are important concerns that affect the consumer's online shopping experience.[21] In order to enable this, stakeholders within the digital payment ecosystem need stable and convenient access to payment details, including card information.

2. Assessing the proposed solution: Tokenisation

The ability to store card details is important for stakeholders in the payment ecosystem for business interests and continuity. However, there have been instances where the details are leaked due to a breach of security. In order to facilitate CoF while mitigating the security risks,

[19] PwC Global (2021), '*A time for hope: Consumers' outlook brightens despite headwinds'*, PricewaterhouseCoopers, Retrieved from https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey.html
[20] DSCI-Paypal (2020), *'Fraud & Risk Management in Digital Payment'*, Retrieved from https://www.dsci.in/sites/default/files/DSCI-PayPal-Report.pdf
[21] Chawla,N. (2021, July 9), *'E-Commerce and Consumer Protection in India: The Emerging Trend'*, Springer, Retrieved from https://link.springer.com/article/10.1007/s10551-021-04884-3

CoFT has been proposed as a solution. Tokenisation has been welcomed by the payments industry as a solution for security breach instances pertaining to card details. However, there are certain concerns relating to implementation and security which must be deliberated upon for effective implementation of this solution. In addition to the anticipated challenges listed below; there may be concerns that will come up once implementation picks up pace; thereby causing uncertainty in the payments ecosystem.

a. Implementation challenges

Concerns due to interdependence of stakeholders

The payments ecosystem, including merchants, PA/PGs, card networks and banks constantly interact to process payments. In order for tokenisation to be effective, it is necessary that every stakeholder in the value chain implements the relevant technological changes[22]. For instance, card issuers are required to provide tokenisation services as Token Service Providers (TSP)s, which includes the ability to tokenise and de-tokenise card data. Additionally, card issuers are required to provide the users a list of merchants he/she has permitted to use CoFT with. Resultantly, merchants are dependent on card issuers establishing effective mechanisms to adhere to the RBI guidelines. It must be noted that implementation of tokenisation is a sequential process. At the very outset, banks and card networks need to make the requisite changes. Until that is done, it will not be feasible for merchants and other downstream entities to implement the system.

Further, various merchants utilize services of PAs for processing transactions through commercial agreements. Thus, the ability of PAs to be seamlessly onboarded on the tokenisation framework of card networks will also affect access of merchants to payment options. Lastly, the RBI guidelines provide that complete compliance with the requirement of not storing card details will be the responsibility of card networks.[23] However, the extent to which networks will be able to enforce the requirement by every stakeholder, including merchants and PAs remains to be seen. Therefore, in order for tokenisation to become an effective norm, it is essential that every stakeholder in the payment ecosystem is able and willing to adopt it.

Internal disruptions

[22] Venkatanarayanan,A. (2021, November 21), *'Winners And Losers Of The Recurring Payments Shake-Up'*, Bloomberg Quint, Retrieved from https://www.bloombergquint.com/opinion/winners-and-losers-of-the-recurring-payments-shake-up
[23] RBI (2021, September 07), *'Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services'*, Reserve Bank of India, Retrieved from https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12159&Mode=0

Tokenisation may cause disruption by either modifying existing mechanisms or necessitating new tasks. To ensure that tokenisation is implemented as a sustainable and secure tool and not merely as a box ticking exercise, stakeholders will need to fulfill certain responsibilities.[24] For instance, TSPs will need to verify that the security of all tokenisation components is in accordance with PCI DSS requirements. In order to ensure effective deployment of the solution, they may need to produce relevant literature for merchants customized for individual requirements.

For merchants, uncertainty over the manner of processing refunds and other transactions to the consumer with tokens instead of card details still looms, necessitating research and deliberations. Additionally, merchants will need to assess whether the TSP solution supports and enforces their security policy requirements and periodically review its interaction with the tokenisation systems to identify unauthorized access. Considering that tokens differ in their nature, process flow and interaction points from plain text data, banks, card networks, PAs/PGs and merchants may need to update incident response systems and disaster recovery plans. These may include strategies for remediation like rejecting de-tokenisation requests from compromised systems, reissuing tokens and re-encrypting data after necessary authorizations.

Therefore, a time-consuming and resource intensive overhaul of internal mechanisms may be required. Merchants with global presence may be able to implement these changes due to their financial strength and experience with tokenisation in foreign jurisdictions. However, smaller merchants active only within India may find the implementation difficult due to limited experience and resources.

b. Security Challenges

Tokenisation is certainly a significant step forward in protection of sensitive details. However, we need to understand the security concerns that may arise despite its implementation. These concerns have not been sufficiently discussed in consultation with relevant stakeholders and experts. For instance, TSPs can adopt either of the two tokenisation methods: tokenisation vaults or vaultless tokenisation. In the former, the service replaces the original data value with a token and stores the original value along with the relevant token inside a file or database. Further, the vault facilitates the ability to tokenise and de-tokenise card data, depending on the requirement.

[24] PCI DSS (2011), '*Information Supplement: PCI DSS Tokenization Guidelines'*, PCI Security Standards, Retrieved from:https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf?agreement=true&t%20ime=1638174774404

In the latter, vaultless tokenisation stores the code in a vault and creates an in-memory codebook of the tokenisation mapping.

Security concerns about tokenisation vaults primarily arise since it creates a copy of the sensitive data and moves it to another location. Rather than effectively securing the data, it creates a single point of attack in tokenisation infrastructure while acting as a high-risk target for data thefts. In a way, tokenisation reduces security risks on the merchant side, but transfers this risk upstream to the acquirer or issuer. The RBI guidelines and PCI DSS standards do not mandate or prohibit the use of token vaults or vaultless tokenisation. Certain existing TSPs internationally[25] and new TSP services in India[26], in fact, utilize token vaults. In the Indian context, the security risks, feasibility and affordability of either of the two approaches has not yet been made.

For generation of multi-use tokens, TSPs often hash sensitive data with a unique salt value per merchant[27]. It has been pointed out that using the same salt for the same merchant can raise security risks. If a malicious individual is able to retrieve the salt and proceeds to conduct a dictionary attack, the payment card information could potentially be recovered.

Further, any cybersecurity framework exists on three pillars - Confidentiality, Integrity and Availability[28]. Research shows that there is a tendency to focus on confidentiality and availability of data while integrity of the data is left unaddressed. However, if the integrity of the data is suspect, then that defeats the purpose of confidentiality and availability. Tokenisation aims at limiting the number of stakeholders who will hold this data. This also means that a dataset won't have any redundancy as well as lack means to arrive at integrity in the event of a major failure. The failure could arise from not only hacking, but also from cascading coding failures.

These are some of the security concerns about tokenisation that require adequate acknowledgment and discussion. Tokenisation is believed to be a significantly more secure method of storing data. However, absence of a comprehensive and intensive risk assessment process of the technology and its potential implications for the Indian payments sector can cause unease among certain stakeholders.

---

[25] Visa team, '*Visa Token Service'*, Visa, Retrieved from https://www.visa.co.in/partner-with-us/payment-technology/visa-token-service.html#1

[26] Razorpay (2021, Oct. 12), *'Decoding Card-on-File Tokenisation: All You Need to Know',* Razorpay, Retrieved from https://razorpay.com/blog/card-on-file-tokenisation-all-you-need-to-know/

[27] Visa (2010, July 14), '*Visa Best Practices for Tokenization 1.0'*, Visa, Retrieved from https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf

[28] Ezer Osei Yeboah-Boateng (2013), *'Cyber-Security, Challenges with SMEs in Developing Economies: 'Issues of Confidentiality, Integrity & Availability (CIA)'* Department of Electronic Systems, retrieved from https://vbn.aau.dk/en/publications/cyber-security-challenges-with-smes-in-developing-economies-issue

V. WAY FORWARD

While CoFT is a good option to secure payments and maintain convenience of CoF, it is important that tokenisation is implemented only after resolving all loose ends. The idea behind preventing merchants to store data is the increasing number of data and cybersecurity thefts in the past year. As highlighted earlier, the RBI's primary concern is that leakage of CoF data can have serious implications on the security of the cardholders data. This is especially true since many jurisdictions do not require AFA for card transactions, and this card data can also be misused to commit fraud through social engineering techniques.[29] The RBI took note of past incidents where card data stored by some merchants have been compromised/leaked.[30] Further, it seems that the RBI wants to bring organisations with rapid rates of growth under the ambit of regulation.

Previously, the Wattal[31]*Committee on Digital Payment* and Nilekani[32] Committee that produced the *Report of the High Level Committee on Deepening of Digital Payments* have also identified behavioral and demographic aspects like literacy as potential reasons for payment frauds. Therefore, it is important that the approach towards ensuring payment security looks at technological limitations, behavioral aspects and demographic factors holistically.

The central issue is that of implementation timelines. The period of three to four months for creation, testing, rolling out, integrating and implementing tokenisation is unrealistic, considering tokenisation requires significant changes on the part of card issuers as well as other stakeholders including merchants, aggregators, gateways and banks. It must be noted that in various countries, CoF and tokenisation coexist, and India should consider taking that approach. If not, we must ensure that (a) there is enough time to test and roll it out to consumers, and (b) the solution is scalable to millions of transactions per second, with at least 85% success rates (like cards) across multiple use cases (like EMIs, recurring, offers, refunds etc.).

Industry experts opine that a major gap exists in the overall ecosystem readiness and execution,

---

[29] RBI (2021, September 7), *'Tokenisation of Card Transactions – Enhancements'* Reserve bank of India, Retrieved from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52188
[30] *Ibid.*
[31] Watal,R.P., et.al. (2016) , *Committee on Digital Payment*, Ministry of Finance, Retrieved from https://dea.gov.in/sites/default/files/watal_report271216.pdf
[32] Committee on Deepening of Digital Payments (2019 May) *Report of the High Level Committee on Deepening of Digital Payments*, Reserve Bank of India, Retrieved from https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CDDP03062019634B0EEF3F7144C3B65360B280E420AC.PDF

causing disruption. While other countries do not mandate CoFT, it has been accepted by stakeholders in their payment ecosystems, since it proves to be a more secure experience.

To emphasise the interconnectedness of the ecosystem, it is important to understand the transaction chain. To begin with, a customer inputs their card details on the merchant's website. Now these card credentials will be sent to the merchant's payment service provider. In turn, the service provider will send this information to PGs linked with the acquirer bank, who then share this with the card network. Hence, the tokenisation framework must be put in place for each of the aforementioned stakeholders within the given timeframe, making the proposed implementation particularly difficult.

To ensure a more seamless transition towards the new system, the key recommendations of the paper may be considered. These recommendations have been further explained below.

1. **Extending the Deadline**

As highlighted above, the current 31st December, 2021 timeline is too short for implementing the tokenisation framework which was permitted only on 7 September 2021. If we need to enforce any of the rules in the market, there is a need to ensure all the parties involved are making necessary changes, as any non compliance on part of one of the parties would impact the overall payment ecosystem and would cause immense harm to consumers. All the stakeholders in the ecosystem have to be equipped to implement the framework, including small banks and businesses. Extending the deadline by at least six months would be beneficial for the ecosystem. While established organisations may be able to implement the tokenisation system, there is also a need to consider smaller merchants who have to tie up with the aggregators to enable their payment systems.

Based on our primary research as well, interviewees were of the opinion that the current timeline is very difficult to adhere to for a smooth transition. **Stakeholders need time to assess and address any complexity in implementing this framework before CoF details are permanently deleted.** There is a need to consider that the services are available to all the merchants, banks etc. All five card networks operating in the country have to be ready with this system. This requires a significant transition for the ecosystem and any loose ends would result in disruption. There is a need to ensure that the necessary processes on the merchant's and card issuer's end are in place before moving forward with the implementation.

2. **Phased Implementation and Auditing**

To ensure smooth implementation of the proposed systems and to avoid consumer and merchant inconvenience, the RBI could consider implementing the said framework in a phased manner with auditing for its regulated entities at each distinct stage. A phased programme could be designed to be implemented over a course of six months, where the RBI audits every bank and card network primarily to ensure that their systems are in place for the seamless flow of transactions. **Taking note from the e-mandate regulation that came into force this October, the RBI may consider replacing the CoF system only when the new system is properly functioning.**

Further, phased implementation would also enable stakeholders to easily identify and resolve pain points. This would give them sufficient time to identify the issues, points of failure and to resolve issues at an ecosystem level. For example - refunds could be seen as one of the potential pain points. It needs to be kept in mind that tokenisation does not have a deadline as such, but the deadline is for merchants and aggregators to delete CoF data. For example, if CoF tokenisation is not implemented fully by December 31, 2021, a merchant would find it extremely difficult to initiate refunds if they do not have CoF data with them.

3. **Analyzing security standards for stakeholders**

Considering the scale and ambitions of the country's digital payments sector, it is imperative that the security standards being implemented are analysed sufficiently. As illustrated above, tokenisation may cause security concerns by transferring financial data to a secure vault. Therefore, introduction of additional layers of security and including encouragement of vaultless tokenisation is suggested. Further, the aforementioned CIA framework, and especially the pillar of data integrity, needs to be fully explored before looking at tokenisation as a solution for maintaining data security. The bottom line is that without adequate measures for maintaining data integrity, there can be no security.

Additionally, the RBI could analyse security aspects of vault tokenisation, and come up with a whitepaper on the cybersecurity concerns arising out of implementing repositories of data. The RBI could also look at the advantages and disadvantages associated with ensuring that only those merchants and PAs that are PCI DSS compliant are allowed to store card details. **Further, in order to enable security and uniformity for whosoever stores the card details, the RBI should come up with certain uniform and enhanced security standards under the**

tokenisation framework. This would create an enabling and secure ecosystem as a whole and would also increase the security standards for the merchants.

4. **Adopting a consultative approach for future regulation**

With regards to future regulation, the RBI should aim to adopt a more consultative and transparent approach. Taking lessons from the disruption caused by the e-mandate regulation, the RBI must provide sufficient time and ensure ease of compliance to minimise disruption in the ecosystem while implementing new systems. This is a healthier model to aspire towards, rather than waiting for post implementation non-compliance and retrospective action, which hinders the consumer experience and causes loss of business to merchants and others who are operating on the current system. Another factor that would help the RBI become more transparent is to publish stakeholders' responses, either anonymised or public as RBI deems fit. This would ensure accountability and provide transparency in terms of suggestions made to the regulator.

About the authors

Anand Venkatnarayanan
Strategic Advisor, DeepStrat

Ayush Tripathi
Senior Research Associate, The Dialogue

Gautam Kathuria
Senior Research Associate, The Dialogue

Saksham Malik
Senior Research Associate, The Dialogue

Recommended Citation: Anand V, Ayush T, Gautam K, Saksham M, (December 2021), RBI's CoF and Tokenisation Guidelines-Analysing the Potential Impact on Digital Payments Industry, New Delhi, The Dialogue and DeepStrat.

**The Dialogue has been ranked as the world's Top 10 think-tanks, for second consecutive year, to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania, the leading body that recognises the work o3f think-tanks globally, in their 2021 rankings.*

The Dialogue is a public-policy think-tank with a vision to drive a pro-gressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

www.thedialogue.co

Deepstrat is India's leading authority on risk assessment & mitigation, public policy, geo-political risk and conflict resolution. Deepstrat was founded by a group that includes those who served in the top echelons of the Indian govern-ment in fields as diverse as intelligence, policing, military and international relations. Its founding members also include experienced public policy, legal and media professionals who served in leadership roles for decades. Deepstrat facilitates different stakeholders to come together and resolve contentious issues backed by cutting-edge research.