केनरा बैंक Canara Bank

REQUEST FOR QUOTES [RFQ 064/2024-25]

for

Engagement of CERT-IN/CISA Auditor to conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Issued by: **Canara Bank**
Single Tender Enquiry Processing Section
Centralized Procurement & Vendor Management Wing, HO (Annexe)
1st Floor, Naveen Complex
14, M G Road
Bengaluru-560 001
Phone No:080-25584873
Email: singletender@canarabank.com

केनरा बैंक Canara Bank

BID SCHEDULE

Sl. No.	Description	Details
1.	RFQ No. and Date	RFQ 064/2024-25 dated 30/11/2024 for engagement of CERT-IN/CISA Auditor to conduct System Audit for CoFT Compliance Requirement for issuer SAR.
2.	Location Address for submission of Bid/s [Address for Communication]	The Senior Manager Canara Bank, Single Tender Enquiry Processing Section Centralized Procurement & Vendor Management Wing, Head Office (Annexe) 1st Floor, Naveen Complex 14, M G Road Bengaluru -560 001 Karnataka
		Tel - 080-25584873 Email: singletender@canarabank.com
3.	Date of Issue	30/11/2024, Saturday
4.	Last Date of Submission of Bids	21/12/2024, Saturday up to 03:00 PM
5.	Date and Time of Opening Bids	21/12/2024, Saturday at 03:30 PM

केनरा बैंक Canara Bank

Dear Vendor,

The Bank intends to conduct System Audit for CoFT Compliance Requirement for issuer SAR.

1.	**Details of the Audit**	**To conduct System Audit for CoFT Compliance Requirement for issuer SAR.**
2.	**Scope of Work/Technical Requirements**	**As per Annexure-VI**
3.	**Time Lines for completion of audit**	**4 Months from the date of acceptance of PO**
4.	**Warranty Period (If applicable)**	**NA**
5.	**Payment Terms & Conditions**	**As per Annexure -III**
6.	**Bill of Material**	**As per Annexure -II**
7.	**Mode of Submission of Bid/Quote**	**Hard copy or Softcopy** **Softcopy- (Digitally Signed PDF file of the bid which is Password protected should be send to the below mentioned Email ID: singletender@canarabank.com)** **Hardcopy- (The bid should be submitted in sealed cover addressed to the Bank at the below mentioned address within the date and time specified).**
8.	**Bid Submission Due Date & Time**	**21/12/2024, Saturday up to 03:00 PM**
9.	**Other Terms and Conditions**	**As per RFQ 064/2024-25**
10.	**Any Other Information**	**NA**

Yours Faithfully,

Authorized Signatory
Note: For further clarification, if any, please contact us.

The Senior Manager
Canara Bank,
Single Tender Enquiry Processing Section
Centralized Procurement & Vendor Management Wing,
Head Office (Annexe)
1st Floor, Naveen Complex
14, M G Road
Bengaluru -560 001
Ph. No: 080- 25584873.

This bid is restricted to following Bank's empaneled CERT-IN auditors selected through EOI-09/2023-24 dated 19/03/2024.

1. **M/s Digital Age strategies Pvt. Ltd.**
2. **M/s AAA Technologies Pvt. Ltd.**
3. **M/s SecurEyes Techno Services Pvt. Ltd.**
4. **M/s AKS Information Technology Services Pvt. Ltd.**

केनरा बैंक Canara Bank

ANNEXURE-I

1. **Objective:**

   The Bank seeks to establish a highly professional relationship with the auditor responsible for conducting System Audit for CoFT Compliance Requirement for issuer SAR.

2. **Requirement Details:**

   Bank invites online submission of bids from Cert-In empaneled auditors for conducting System Audit for CoFT Compliance Requirement for issuer SAR in Canara Bank as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document.

3. **Project Timelines:**

   Bidders are requested to keep the following timelines with regard to the completion of Assessment.

   - The complete activity System Audit for CoFT Compliance Requirement and submission of Final report) has to be completed in 4 months from the date of issue of Purchase Order.

4. **Penalties & Liquidated damages on delay in completion of Assessment:**

   If the assessment is not completed within the timelines, Bank may be entitled to charge penalty @0.50% on delay per week or part there of on the total cost of the Assessment. However, the total Penalty/LD to be recovered shall be restricted to 5% of total cost of the Assessment (exclusive of Taxes).

5. **Subcontracting:**

   The vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.

6. **Deliverables:**

   i. Audit reports should be provided to Bank after completion of the subject assessment in PDF & Excel format along with Two hard copies (optional, if required).

   ii. Email and Phone support till final closure report is to be provided by the Auditor.

We comply with each point mentioned above without any deviations.

Date:	Signature with seal Name: Designation:

केनरा बैंक Canara Bank

ANNEXURE-II

Bill of Material

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 064/2024-25 dated 30/11/2024.

[Amount in INR]

Sl. No	Audit	Cost Price			
		Price (Excl. of Tax)	Tax for Column A		Price (Incl. of Tax)
		A	B% of tax	C Tax Amt.	D=A+C
1.	To conduct System Audit for CoFT Compliance Requirement for issuer SAR as per Scope of Work mentioned in RFQ-064-2024-25 dated 30/11/2024	-	-	-	-

Date:	Signature with seal Name: Designation:

केनरा बैंक Canara Bank

ANNEXURE-III

Payment Terms & Conditions

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 064/2024-25 dated 30/11/2024.

1. 100% payment should be released on submission of invoice, Confirmation of work completion from the Card Technology Management section, Credit & Prepaid Cards Wing, HO.
2. Bank will not pay any amount in advance.
3. Audits are to be conducted onsite only and Remote access cannot be provided.
4. Bidder should employ the resources for the System Audit.
5. The payments will be released through NEFT/RTGS and the selected bidder has to provide necessary bank details like account number, bank's name with branch name, Correct IFSC code etc.

Locations details are as mentioned below: Location for conducting audit is from onsite only at the following location of the Bank.

Sl. No	Section / Wing	Location
1.	CTM Section, Credit & Prepaid Cards Wing	Bengaluru

We comply to all the points mentioned in RFQ, Scope of work, without any deviation.

Date:	Signature with seal: Name : Designation :

केनरा बैंक Canara Bank

ANNEXURE-IV
SCOPE OF WORK

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 064/2024-25 dated 30/11/2024.

A-Validation

Domain	Guideline	Testing criteria	Tokenization type (Device/CoFT/Device and CoFT)	Card Issuer	Token requestor / merchant	Token service provider	Acquirer	Others	Remarks
Registration by customer	All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Miscellaneous	No charges should be recovered from the customer for availing this service.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Unique token	The token shall be unique for a combination of card, token requestor and device (referred hereafter as “identified device”).	To be validated	Device		Y	Y			For token requestors validation should be done to check if unique tokens are assigned to merchants.
Tokenization – de-tokenization service	Tokenisation and de-tokenisation shall be performed only by the authorised card network	To be validated	Device and CoFT			Y			
Tokenization – de-tokenization service	Recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only.	To be validated	Device and CoFT			Y			

Tokenization – de-tokenization service	Adequate safeguards shall be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times. *Note: This control must be tested by auditors for banks that receive and store the tokens from CPN. Please specifically call out if the bank has access to the token and/or is storing the token.*	To be validated	Device and CoFT	Y		Y		Y	Applicable for card networks and entities (e.g. issuers) that may store both PAN and token Note: Issuers should store only store the masked PAN received from the networks. A check must be done to validate the same.
Tokenization – de-tokenization service	Tokenization and de-tokenization requests should be logged by the card network and available for retrieval, if required.	To be validated	Device and CoFT			Y			Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Tokenization – de-tokenization service	Actual card data, token and other relevant details shall be stored in a secure mode. *Note: Auditor must specify any and every card information such as card expiry, cardholder name etc. being stored by the token service participant.*	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Tokenization – de-tokenization service	Token requestors shall not store PAN or any other card detail.	To be validated	Device and CoFT		Y				
Certification of systems of card issuers /acquirers, token requestors and their app, etc.	Card network shall get the token requestor certified for (a) token requestor's systems, including hardware deployed for this purpose, (b) security of token requestor's application, (c) features for ensuring authorised access to token requestor's app on the identified device, and (d) other functions performed by the token entity, including customer onboarding, token provisioning and storage, data storage, transaction processing, etc.	To be validated	Device and CoFT		Y	Y			While the point is to be exclusively tested for card networks, Auditors reviewing token requestors must validate if such certification is undertaken actively by these entities.

Certification of systems of card issuers /acquirers, token requestors and their app, etc.	Card networks shall get the card issuers / acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenized card transactions by them.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	While the point is to be exclusively tested for card networks, auditors reviewing other entities (card issuers / acquirers, their service providers and any other entity) must validate if such certification is undertaken actively by these entities.
Certification of systems of card issuers /acquirers, token requestors and their app, etc.	Card network shall ensure that certification of systems of card issuers / acquirers, token requestors and their application shall conform to international best practices / globally accepted standards.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	While the point is to be exclusively tested for card networks, auditors reviewing other entities must validate if such certification is undertaken actively by these entities.
Registration by customer	Registration of card on token requestor's app shall be done only with explicit customer consent through Additional Factor of Authentication (AFA), and not by way of a forced / default / automatic selection of check box, radio button, etc.	To be validated	Device and CoFT		Y	Y		Y	Applicable to issuers only if they are offering an application through which cardholders can tokenize cards

Registration by customer	AFA validation during card registration, as well as, for authenticating any transaction, shall be as per extant Reserve Bank instructions for authentication of card transactions. Note: *The auditor must validate AFA for sample cases including only tokenization, tokenized card transaction and tokenization + transaction.*	To be validated	Device and CoFT	Y		Y			
Registration by customer	Customers shall have option to register / de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.	To be validated	Device		Y				Applicable for device token requestors having a customer facing application. Applicable to issuers only if they are offering an application through which cardholders can tokenize cards
Registration by customer	Customers shall be given option to set and modify per transaction and daily transaction limits for tokenized card transactions.	To be validated	Device and CoFT	Y					
Registration by customer	Suitable velocity checks (i.e., how many such transactions will be allowed in a day / week / month) may be put in place by card issuers / card network as considered appropriate, for tokenized card transactions.	To be validated	Device and CoFT	Y					
Registration by customer	For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.	To be validated	Device and CoFT		Y				Applicable for token requestors having a customer facing application Applicable to issuers only if they are offering an application through which cardholders can tokenize cards

Secure storage of tokens	Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.	To be validated	Device and CoFT		Y				Applicable for token requestors
Customer service and dispute resolution	Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorized usage.	To be validated	Device	Y					Applicable for card issuing entities
Customer service and dispute resolution	Card network, along with card issuers and token requestors, shall put in place a system to immediately deactivate unauthorized/exposed tokens and associated keys.	To be validated	Device and CoFT	Y	Y	Y			Applicable for card networks, issuing entities and token requestors
Customer service and dispute resolution	Dispute resolution process shall be put in place by card network for tokenized card transactions.	To be validated	Device and CoFT			Y			Applicable for card networks
Safety and security of transactions	Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified device".	To be validated	Device and CoFT			Y			Applicable for card networks
Safety and security of transactions	Card network shall: a) ensure monitoring to detect any malfunction, anomaly, suspicious behaviour, or the presence of unauthorized activity within the tokenization process and; b) implement a process to alert all stakeholders.	To be validated	Device and CoFT			Y			Applicable for card networks
Safety and security of transactions	Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.	To be validated	Device and CoFT	Y					Applicable for card issuers
Tokenization – de-tokenization service	Card issuers can offer card tokenisation services as Token Service Providers .	To be validated	Device and CoFT	Y					Applicable for Token service providers
Tokenization – de-tokenization service	The facility of tokenisation shall be offered by the Token Service Providers only for the cards issued by / affiliated to them.	To be validated	Device and CoFT			Y			Applicable for Token service providers. Applicable to card issuers only if they create

									tokens (tokenize and detokenize cards).
Tokenization – de-tokenization service	The ability to tokenise and de-tokenise card data shall be with the same Token Service Providers.	To be validated	Device and CoFT			Y			Applicable for Token service providers. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Registration by customer	Tokenisation of card data shall be done with explicit customer consent requiring Additional Factor of Authentication (AFA) validation by card issuer.	To be validated	Device and CoFT	Y	Y	Y			
Transaction tracking/ reconciliation	For transaction tracking and / or reconciliation purposes, entities can store limited data – last four digits of actual card number and card issuer's name – in compliance with the applicable standards.	To be validated	Device and CoFT		Y		Y	Y	Applicable for all entities except issuers and card networks
Unique token	For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant	To be validated	CoFT		Y	Y			Applicable for card networks. Additionally for token requestors validation should be done to check if unique tokens are assigned to merchants. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Registration by customer	If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then AFA validation may be combined.	To be validated	Device and CoFT	Y		Y			Applicable to card issuers and networks

Token de-registration	The merchant shall give an option to the cardholder to de-register the token.	To be validated	Device and CoFT		Y				Applicable to merchants and token requestors that have a customer facing application
Token de-registration	Further, a token requestor having direct relationship with the cardholder shall: a) list the merchants in respect of whom the CoFT has been opted through it by the cardholder b) provide an option to deregister any such token	To be validated	CoFT		Y				
Token de-registration	a) A facility shall also be given by the card issuer to the cardholder to view the list of merchants in respect of whom the CoFT has been opted by her / him, and to deregister any such token. b) This facility shall be provided through one or more of the following channels – mobile application, internet banking, Interactive Voice Response (IVR) or at branches / offices.	To be validated	CoFT	Y					
Registration by customer	Whenever a card is renewed or replaced, the card issuer shall seek explicit consent of the cardholder for linking it with the merchants with whom (s)he had earlier registered the card.	To be validated	CoFT	Y					
Unique token	The Token service provider shall put in place a mechanism to ensure that the transaction request has originated from the merchant and the token requestor with whom the token is associated.	To be validated	CoFT			Y			Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Miscellaneous	In addition to tokenization, industry stakeholders may devise alternate mechanism(s) 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 involves / requires storage of CoF data by entities other than card issuers and card networks. *Note: Auditors must test specific samples for above cases.*	To be validated	Device and CoFT		Y	Y	Y		

CoF data purging	It has been decided to extend the timeline for storing of CoF data by three months, i.e., till September 30, 2022, after which such data shall be purged. There shall be no change in the effective date of implementation of the requirements – all entities, except card issuers and card networks, shall purge the CoF data before October 1, 2022. With effect from October 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store CoF data, and any such data stored previously shall be purged.	To be validated	Device and CoFT		Y		Y	Y	
Guest checkout transactions	Only for guest checkout transaction - a) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+2 days ("T" being the transaction date) or till the settlement date, whichever is earlier. b)This data shall be used only for settlement of such transactions, and must be purged thereafter.	To be validated	Device and CoFT		Y			Y	
Guest checkout transactions	a) The acquiring banks shall not store CoF data for guest checkout transactions beyond a period of T+180 days ("T" being the transaction date). b) For such transactions processed before the April 21,2023, compliance with the T+180 days' timeline shall be ensured by June 30, 2023. c) Additionally, only acquiring banks are permitted to store actual card details used for guest checkout transaction (historical) in offline storing mediums.	To be validated	Device and CoFT				Y		
Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by January 31, 2024	To be validated	Device and CoFT	Y	Y	Y	Y	Y	

Extension to other devices	The scope of tokenization has been extended to include consumer devices – laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc. All other provisions of the circular referred to above shall continue to be applicable.	To be validated	Device	Y	Y	Y	Y	Y	
Enable tokenization through card issuing banks	Does the card issuing entity provide CoF tokens option for multiple merchants through mobile/internet banking channels? (note: Issuing bank may/may not issue tokens in order to provide this feature) a) CoFT generation shall be done only on explicit customer consent, and with AFA validation. If the cardholder selects multiple merchants for which to tokenise his/her card, AFA validation may be combined for all these merchants. b) The tokens thus generated shall be made available on the merchant's payment page, in the cardholder's account with the merchant. c) The cardholder may tokenise the card at any time of his convenience, either on receipt of the new card or later. d) The card issuer shall provide a complete list of merchants for whom it can provide tokenisation services. The cardholders shall select the merchants with whom he/she wishes to maintain tokens. (Alternatively – "The cardholder can make his selection from the list"). e) The card token so issued may be either by the card network or the issuer or both.	To be validated	CoFT	Y		Y			Control is applicable only if the Issuer provides this service. Issuer may or may not act as a token service provider for this to be tested
India Data localization	1. All system providers (entities involved in payment lifecycle) shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	

	2. No payment data element pertaining to the end-to-end payment string can be stored abroad in any form, including hashed, masked, encrypted or tokenized.								
Token access	Does the card issuer have access to token number (Device and/or CoFT) during any stage of transaction processing ? Evidence must be captured appropriately for validation.	To be validated	Device and CoFT	Y					Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted
Token storage	Does the card issuer store token number (Device and/or CoFT) during or after the transaction processing ? Evidence must be captured appropriately for validation.	To be validated	Device and CoFT	Y					Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted
Single token	How did the auditor validate if unique IDs are assigned to each end merchant on-boarded by the TR? How is it ensured that these unique IDs created for each end merchant are also tagged to the initiation of separate token requests for each merchant?	To be validated	CoFT		Y				
Single token	Does the TR utilize token generated for merchant A in place of merchant B? If no, how is the same ensured.	To be validated	CoFT		Y				

	Case A : For cases where entity requests/processes CoF Token transactions for merchants including their sister merchant entities - Validate whether a unique token is requested/utilized for each merchant (including distinct merchants who may be sister companies or group companies) during creation and subsequent tokenized transaction requests. Note: For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant. The word "merchant" wherever used in the mentioned circular refers to the end-merchant. However, in case of an e-commerce marketplace entity, merchant refers to the said e-commerce entity. Further, token requestor and merchant may or may not be the same entity.	To be validated	CoFT		Y				e.g. if entity is processing transactions for a large conglomerate, business group with multiple businesses e.g. telecom, DTH, Bank, Wallet, Streaming, etc., are distinct tokens been provisioned for transactions at each of these merchants (each business within the conglomerate, business group?)
	Case B : For cases where entity requests/processes CoF Token transactions for any of their own sister/group companies: Validate whether a unique token is requested/utilized for each group/sister entity (legal entity) during creation and subsequent tokenized transaction requests. Note: For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant. The word "merchant" wherever used in the mentioned circular refers to the end-merchant. However, in case of an e-commerce marketplace entity, merchant refers to the said e-commerce entity. Further, token requestor and merchant may or may not be the same entity.	To be validated	CoFT		Y				e.g. if entity is processing transactions for two sister entities on your mobile app/website where Sister entity A provides telecom services and Sister entity B provides prepaid wallet (wallet load transactions) for the same card, have distinct tokens been provisioned for transactions at each of these entities (merchants)?

B-Information Control:

TSP auditor is required to consider and cover the below informational controls during the audit and include the same in the report.

Sr No	Guideline Date	Para/section	RBI document name	RBI document number	Domain	Guideline
1	08-Jan-19	Leading paragraph	Tokenization – Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenization in card transactions for a specific use case. For the present, this facility shall be offered through mobile phones / tablets only. Its extension to other devices will be examined later based on experience gained.
2	08-Jan-19	Point 2	Tokenization – Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Permission to tokenize	It has now been decided to permit authorised card payment networks to offer card tokenization services to any token requestor (i.e., third party app provider), subject to the conditions listed in Annex 1.
3	08-Jan-19	Point 2	Tokenization – Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.).
4	08-Jan-19	Point 4	Tokenisation – Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	All other instructions related to card transactions shall be applicable for tokenised card transactions as well. The ultimate responsibility for the card tokenisation services rendered rests with the authorised card networks.

5	08-Jan-19	Point 6 and 7	Tokenisation – Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	- Before providing card tokenisation services, authorised card payment networks shall put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenisation services to customers. - This system audit shall be undertaken by empanelled auditors of Indian Computer Emergency Response Team (CERT-In) and all related instructions of Reserve Bank in respect of system audits shall also be adhered to. - A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, if any, from the conditions listed in Annex 1, along with the compliance thereto. - Further, a report on the details provided in Annex 2 shall be submitted at monthly intervals to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai and by email. -This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).
6	07-Sep-21	3.a	Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	On a review of the tokenisation framework and to enable cardholders to benefit from the security of tokenised card transactions as also the convenience of CoF, it has been decided to effect the following enhancements: a) Extend the device-based tokenisation framework referred to at paragraph above to CoF Tokenisation (CoFT) as well.
7	07-Sep-21	3.f	Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	References	Additional requirements relating to CoFT are listed in the Annex.
8	07-Sep-21	4.a	Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	CoF data purging	With effect from January 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store the actual card data. Any such data stored previously shall be purged.
9	07-Sep-21	4.c	Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Monitor compliance	Complete and ongoing compliance with the above by all entities involved, shall be the responsibility of the card networks.

10	07-Sep-21	Annex 7 and 8	Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Conditions to be fulfilled for offering CoFT services	All other provisions of the RBI circulars dated January 8, 2019 and August 25, 2021 shall be applicable. The TSPs shall monitor and ensure compliance in this regard.
11	23-Dec-21	Point 2.a	Restriction on storage of actual card data [i.e. Card-on-File (CoF)]	RBI/2021-2022/142 CO.DPSS.POLC.No.S-1211/02-14-003/2021-22	CoF data purging	The timeline for storing of CoF data is extended by six months, i.e., till June 30, 2022; post this, such data shall be purged;
12	24-Jun-22	Point 3	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S-567/02-14-003/2022-23	Points to note	On a review of the issues involved and after detailed discussions with all stakeholders, it is observed that considerable progress has been made in terms of token creation. Transaction processing based on these tokens has also commenced, though it is yet to gain traction across all categories of merchants. Further, an alternate system in respect of transactions where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as "guest checkout transactions") has not been implemented by the industry stakeholders, so far.
13	28-Jul-22	Point 3.b.i	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	For cases where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as "guest checkout transactions"), the following are being permitted as an interim measure – i) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+4 days ("T" being the transaction date) or till the settlement date, whichever is earlier. This data shall be used only for settlement of such transactions, and must be purged thereafter.
14	28-Jul-22	Point 3.b.ii	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	For handling other post-transaction activities, acquiring banks can continue to store CoF data until January 31, 2023.
15	28-Jul-22	Point 4	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Non-compliance measures	Appropriate penal action, including imposition of business restrictions, shall be considered by the RBI in case of any non-compliance.

16	21-Apr-23	Point 3c	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-2024	Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by October 31, 2023
17	11-Feb-22	2.ii	Tokenisation – Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	The auditors assessing CPNs' tokenisation set-up shall also assess whether adequate controls are put in place to ensure certification of tokenisation setup of token service participants.
18	11-Feb-22	2.iii	Tokenisation – Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	a) The system audit report (SAR) submitted by token service participants must contain item-wise compliance status on each requirement specified in extant guidelines on tokenisation services issued by RBI. b) The auditors of a CPN shall also examine the SARs of token service participants to ensure that relevant areas are covered in the audit. Any observation raised in the SARs shall be tracked by the CPNs for timely closure.
19	11-Feb-22	3	Tokenisation – Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	a) As regards the tokenisation SAR of CPNs submitted to RBI, the report must contain item-wise response from the auditors on each requirement specified in the above as well as other relevant circulars. b) In case the CPN offers Card-on-File Tokenisation (CoFT), item-wise compliance status for related RBI instructions shall also be specified in the SAR. Further, the report shall contain a certificate issued by the auditors, indicating the deficiencies observed in the SARs of token service participants.
20	11-Feb-22	2.i.	Tokenisation – Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	It is the responsibility of an authorised CPN to ensure that the token requestors and any other participants (cumulatively termed as token service participants, hereafter) involved in providing its card tokenization services to customers, adhere to RBI instructions on card tokenization, data storage, system audit and other relevant instructions.

Date :

Signature with seal
Name:
Designation: