भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/2025-26/79
CO.DPSS.POLC.No. S 668/02-14-015/2025-2026 September 25, 2025

Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025

Index

1. Introduction

All digital payment transactions in India are required to meet the norm of two factors of authentication. While no specific factor was mandated for authentication, the digital payments ecosystem has primarily adopted SMS-based One Time Password (OTP) as the additional factor.

As announced in Statement on Developmental and Regulatory Policies dated February 08, 2024, in order to enable the payments ecosystem to leverage the technological advancements for implementing alternative authentication mechanisms, it has been decided to publish **Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025 (hereinafter referred to as "Directions")**. The directions provide the broad principles which shall be complied with by all the participants in the payment chain, while using a form of authentication.

While these directions are applicable only to domestic transactions, in order to provide a similar level of safety for online international transactions undertaken using cards issued in India, the directions also incorporate necessary instructions for specific cross-border card transactions, in line with the Statement on Developmental and Regulatory Policies dated February 07, 2025.

These directions are issued under Section 18 read with Section 10(2) of the Payment and Settlement Systems (PSS) Act, 2007 (Act 51 of 2007).

2. Short title

These directions shall be called Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025

3. Effective Date

All Payment System Providers and Payment System Participants, including banks and non-bank entities, shall ensure compliance with these directions by April 01, 2026, unless indicated otherwise for any specific provision herein.

4. Applicability

a. These directions shall be applicable to all Payment System Providers and Payment System Participants (banks and non-banks).
b. These directions apply to all domestic digital payment transactions, unless specifically exempted otherwise.

5. Definitions

I. Unless the context otherwise requires, the following terms shall bear the meanings assigned to them as below:

a. **Authentication**: Process of validating and confirming the credentials of the customer who is originating the payment instruction.

b. **Card Not Present (CNP) transaction**: A transaction where the card and acceptance infrastructure are not present in close proximity while making the transaction.

c. **Card Present transaction**: A transaction that is carried out through the physical use of card at the point of transaction.

d. **Cross-border CNP transaction:** A payment instruction wherein the card, issued by an Indian issuer, is used for undertaking a payment transaction favouring a merchant acquired by an overseas acquirer. For such transactions, outflow of foreign exchange is envisaged.

e. **Digital Payment Transaction** shall have the same meaning as “Electronic Funds Transfer” as defined in the PSS Act, 2007.

f. **Factor of Authentication**: Credential of the customer which is used for authentication. The factors of authentication can be from “something the user has”, “something the user knows” or “something the user is” and may comprise, *inter-alia*, password, SMS based OTP, passphrase, PIN, card hardware, software token, fingerprint, or any other form of biometrics (device native or Aadhaar based).

g. **Issuer**: A bank or a non-bank that maintains the customer's account from which payment is made, such as a deposit account or a credit line or a prepaid instrument.

II. Words and expressions used but not defined in these directions and defined in the PSS Act, 2007 shall have the meanings assigned to them in that Act.

6. Principles for authentication of digital payment transactions

The technology and process deployed for authenticating a payment instruction by the Payment System Provider / Payment System Participant(s) shall comply with the following principles:

a. Minimum two factors of authentication

All digital payment transactions shall be authenticated by at least two distinct factors of authentication as defined in paragraph-5(f), unless exempted. The list of exemptions which are currently in force are listed in **Annexure-1**.

Note - Issuers may, at their discretion, offer a choice of authentication factors to their customers in compliance with these directions.

b. At least one of the factors to be dynamic

It shall be ensured that for digital payment transactions, other than card present transactions, at least one of the factors of authentication is dynamically created or proven, i.e., the proof of possession of the factor, being sent as part of the transaction, is unique to that transaction.

c. Robust

The factor of authentication shall be such that compromise of one factor does not affect reliability of the other.

7. Interoperability / Open Access

System Providers and System Participants shall offer authentication or tokenisation service that is accessible to all the applications / token requestors functioning in that operating environment for all use cases / channels or token storage mechanisms.

Note –

i. Operating environment includes device hardware, operating system, etc.

ii. The terms, 'tokenisation','token requestor', 'use cases/channels' and 'token storage mechanisms' shall have the same meaning as assigned to them in the RBI directions on "Tokenisation – Card Transactions" dated January 08, 2019, as amended from time to time.

8. Risk based approach

Issuers may, in line with their internal risk management policies, identify transactions for evaluation against behavioural / contextual parameters such as transaction location, user behaviour patterns, device attributes, historical transaction profile, etc. Based on the perceived risk associated with the transaction, additional checks beyond the minimum two-factor authentication may be resorted to. Issuers may also explore using DigiLocker as a platform for notification and confirmation for high-risk transactions.

9. Responsibility of the issuer

a. An issuer shall ensure the robustness and integrity of the authentication mechanism before deployment.

b. If any loss arises out of transactions effected without complying with these directions, the issuer shall compensate the customer for the loss in full without demur.

c. Issuers shall ensure adherence to the provisions of Digital Personal Data Protection Act, 2023.

10. Cross-border transactions

a. The directions outlined above is not applicable to cross-border digital payment transactions. However, card issuers shall, by October 01, 2026, put in place a mechanism to validate non-recurring, cross-border card not present (CNP) transactions, where request for authentication is raised by an overseas merchant or overseas acquirer. To ensure compliance, card issuers shall register their Bank Identification Numbers (BINs) with card networks.

b. Further, a risk-based mechanism for handling all cross-border CNP transactions shall also be put in place by card issuers by October 01, 2026.

11. Repeal

The list of circulars / directions that are repealed are listed in **Annexure-2**.

Annexure-1

*(Reference: CO.DPSS.POLC.No. S 668/*02-14-015*/2025-2026 dated September 25, 2025)*

Existing exemptions from the requirement of at least two factors of authentication under paragraph-6(a) of these directions. Any subsequent additions / modifications made, from time to time, will also be applicable.

S. No.	Use case	Existing directions
1.	Small-value Contactless Card transactions	*DPSS.CO.PD No.752/02.14.003/2020-21 dated December 04, 2020*
2.	Recurring transactions (other than the first) under the e-mandate framework	*DPSS.CO.PD.No.447/02.14.003/2019-20 dated August 21, 2019* *DPSS.CO.PD No.754/02.14.003/2020-21 dated December 04, 2020* *CO.DPSS.POLC.No.S-882/02.14.003/2023-24 dated December 12, 2023*
3.	Select Prepaid Instruments such as PPI-MTS and Gift PPIs	*CO.DPSS.POLC.No.S-479/02.14.006/2021-22 dated August 27, 2021*
4.	NETC transactions	*DPSS.CO.PD No.1227/02.31.001/2019-20 dated December 30, 2019*
5.	Small value digital payments in offline mode	*CO.DPSS.POLC.No.S1264/02-14-003/2021-2022 dated January 03, 2022*
6.	Travel booking involving Global Distribution System / IATA through commercial / corporate cards.	Letter dated April 17, 2012 (DPSS.CO.PD.No.1910/02.14.003/2011-12) issued to Indian Bank's Association

Annexure-2

(Reference: CO.DPSS.POLC.No. S 668/02-14-015/2025-2026 dated September 25, 2025)

List of circulars / directions that are repealed:

No	Circular No.	Date	Subject
1.	RBI/DPSS No. 1501/02.14.003/2008-2009	February 18, 2009	Credit/Debit Card transactions- Security Issues and Risk mitigation measures
2.	RBI/DPSS No. 2303/02.14.003/2009-2010	April 23, 2010	Credit/Debit Card transactions- Security Issues and Risk mitigation measures for IVR transactions
3.	RBI/DPSS No.914/02.14.003/2010-2011	October 25, 2010	Credit/Debit Card transactions- Security Issues and Risk mitigation measures for Card Not Present Transactions
4.	DPSS.CO.No.1503/02.14.003/2010-2011	December 31, 2010	Security Issues and Risk mitigation measures related to Card Not present transactions
5.	DPSS. CO. PD 2224/02.14.003/2010-2011	March 29, 2011	Security Issues and Risk mitigation measures - Online alerts to the cardholder for usage of credit/debit cards
6.	DPSS.PD.CO. No.223/02.14.003/2011-2012	August 04, 2011	Security Issues and Risk mitigation measures related to Card Not Present (CNP) transactions
7.	DPSS.PD.CO. No.371/02.14.003/2014-2015	August 22, 2014	Security Issues and Risk mitigation measures related to Card Not Present (CNP) transactions
8.	DPSS.CO.PDNo.1431/02.14.003/2016-17	December 06, 2016	Card Not Present transactions – Relaxation in Additional Factor of Authentication for payments upto ₹2,000/- for card network provided authentication solutions