KPMG

Point of view on Reserve Bank of India (RBI)

Authentication Mechanisms For Digital Payment Transactions Directions, 2025

KPMG. Make the Difference.

Key takeaways from the RBI directions

RBI released directions on authentication mechanisms for digital payment transactions (RBI/2025-26/79 CO.DPSS.POLC.No. S 668/02-14-015/2025-2026 via a notification on 25 September 2025.

All digital payment transactions in India are required to authenticate via two factors of authentication (2FA)

1 April 2026

Is the effective date of compliance for all **Payment System Providers** and **Payment System Participants**, including banks and non-bank entities, unless exempted.

Principles for 2FA authentication

Minimum two factors of authentication
First factor – customer credentials
Second factor - "something the user has", "something the user knows" or "something the user is"

At least one of the factors to be dynamic
For digital payment transactions (excluding card present transactions) – at least one factor should be dynamic in nature, i.e. unique proof of possession

Robust
Compromise of one factor should not affect reliability of the other

Examples of factors of authentication

- SMS based OTP
- Passphrase
- PIN
- Card hardware
- Software token
- Fingerprint
- Other biometrics - (device native or Aadhaar based).

Other Key Requirements

Interoperability / Open Access –
offer services such as tokenisation to all token requestors for all use cases or channels

Risk based approach –
issuers shall also perform fraud risk management for suspicious transactions

Responsibility of the issuer –
to ensure integrity of authentication mechanism, compensate customer in case of any loss, comply with DPDP Act 2023

Cross-border transactions

These directions are not applicable to cross-border digital payment transactions

However, card issuers are required to (by **1 October 2026**), to validate non-recurring, cross-border **card not present transactions**, where authentication request is raised by **overseas** merchant / acquirer

Exceptions

- **Contactless card** small-value transactions
- **E-mandates** (excluding first payment)
- **Prepaid** instruments like Mobile money transfer and gift cards
- **NETC** transactions like FASTag
- **Travel bookings** (global distribution systems) through corporate cards
- **Offline** small-value digital payments

Contributors:

- Aakansha Gupta
- Madhuri Gangaramani

KPMG in India contacts:

Akhilesh Tuteja
Global Head
Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, Head of Function
Digital Trust and Cyber
E: atulgupta@kpmg.com

Kunal Pande
Partner, Leader - Digital Trust & Cyber for FS, Co-Head - Digital Risk & Cyber
E: kpande@kpmg.com

Rohan Padhi
Partner and Co-Lead
Digital Risk and Cloud Security
E: rohanpadhi@kpmg.com

Romharsh Razdan
Partner, Lead Payment Risk and Co-Lead Cloud Security
E: romharsh@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011
Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.