KPMG

Reserve Bank of India (RBI) directive for Aadhaar Enabled Payment System (AePS)

KPMG. Make the Difference.

AePS is a secure payment system that allows customers to carry out basic financial transactions using their **Aadhaar number** and **biometric authentication**. It is facilitated by an AePS Touchpoint Operator (ATO) who is a trained individual that facilitates AePS transactions using Aadhaar authentication in rural areas.

Key risks faced in the AePS lifecycle include:

- Biometric spoofing or cloning
- False positives or negatives
- Misuse by Business Correspondents
- Fraudulent transactions
- Hardware failures of scanners
- Banking system mismatches.

RBI has published a directive to mandate stricter AePS controls

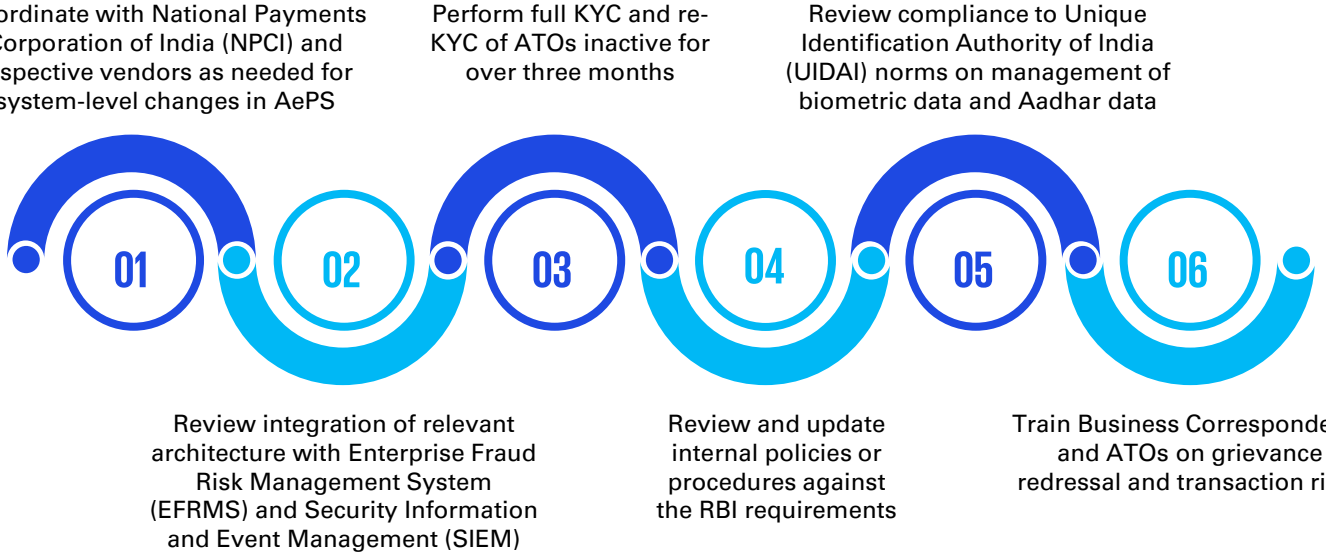
- **Circular issued on 27th June 2025**
- **Enhanced monitoring Of AePS ATMs**
- **Applicable to banks in India and National Payments Corporation of India (NPCI)**

Effective From 1st January 2026

Key Objectives of the Directive

- Banks must implement robust Know Your Customer (KYC) procedures when onboarding ATOs to ensure authenticity and accountability
- Transactions should be continuously assessed based on risk factors like amount, frequency and location
- Operators inactive for more than a period must undergo mandatory re-KYC before resuming services
- Only authorized systems should access AePS services through strictly controlled Application Programming Interface (API)
- Institutions must deploy systems to detect and block suspicious AePS transactions in real time
- Banks must ensure transparency, security, and grievance redressal to build user confidence in AePS

Next Steps for Regulated Entities



How KPMG in India can help

KPMG in India supports banks in meeting adherence to RBI's AePS directives through consulting, implementation assistance and independent reviews of ATO onboarding, KYC processes, fraud controls, and system-level safeguards. We also identify compliance gaps and provide targeted, risk-based recommendations.

Via our collaboration with various regulated entities, banks are supported in strengthening due diligence, enhancing transaction monitoring, and aligning with RBI's 2025 requirements - building trust and resilience across the AePS operations.

Our detailed approach is covered below.

Our four-step approach aligned to CMMI Model in assisting banks to adhere to RBI requirements

Initial

- Understand AePS touchpoints and data flow
- Identify key risks in AePS operations
- Assign responsibility for regulatory adherence.

Managed

- Develop framework in monitoring ATO activity and in identifying inactive ATOs for re-KYC
- Review API security, controls, and the API gateway for AePS.

Defined

- Develop SOPs for onboarding and fraud handling
- Create framework for periodic reviews of ATOs
- Review EFRMS and SIEM use cases.

Optimised

- Prepare dashboards to detect fraud patterns
- Conduct root cause analysis of fraud incidents
- Update compliance frameworks based on regulatory updates.

KPMG in India's key differentiating factors

Our value propositions include:

1. Assisted more than six Indian regulators and quasi-regulators in documenting information security, cyber security, technology review, and digital payments security guidelines.
2. Provided technology consulting services to various kinds of regulated entities such as private and public sector banks, third party application providers (TPAP), insurance companies, and payment gateways/aggregators.
3. Wide range of cyber service line offerings pertaining to cyber strategy, risk, defence, transformation, response, and managed services with robust and experienced team having multiple certifications.

We have conducted various engagements in the digital payments and regulatory space. Below is a snippet of our key clientele:

- **Large multinational bank**
- **Global payment gateway**
- **Indian financial quasi-regulator**
- **Indian public sector client**
- **Indian private sector bank**
- **Large private Indian bank**
- **Global card payment network**
- **Large payment aggregator**

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

Follow us on:
kpmg.com/in/socialmedia