INDIALAW

BANKING AND FINANCE

RBI Mandates KYC and Monitoring of AePS Operators: New Compliance Framework Effective January 2026

AUTHOR Shrishail Kittad, Aditi Rana

PUBLISHED 8 July 2025

Introduction

In a bid to address rising concerns over identity fraud and security vulnerabilities in Aadhaar Enabled Payment System (AePS) transactions, the Reserve Bank of India (RBI), through its directive dated 27 June 2025 (Circular No. CO.DPSS.POLC.No.S339/02-01-001/2025-2026), has introduced a new compliance framework governing due diligence and risk management of AePS operators (ATOs). These directions, issued under the Payment and Settlement Systems Act, 2007, are scheduled to come into effect from 1 January 2026.

This regulatory intervention is aimed at enhancing accountability within last-mile banking agents and ensuring the robustness of authentication-based transactions carried out via Aadhaar. The move follows increasing incidents of fraud, particularly in rural and semi-urban geographies, where Aadhaar-based authentication forms the core of inclusive banking infrastructure.

Legal Framework and Statutory Basis

The regulatory power underpinning this directive is drawn from:

- Section 10(2) and Section 18 of the Payment and Settlement Systems Act, 2007, which empower the RBI to regulate and supervise payment systems in India;
- The circular also harmonises its directions with the Master Direction – Know Your Customer (KYC) Direction, 2016, issued under the Banking Regulation Act, 1949 and the Prevention of Money Laundering Act, 2002;
- Definitions of Aadhaar-related terms refer back to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Together, these legal instruments provide the RBI with both substantive and procedural authority to intervene in authentication-linked banking operations.

Key Compliance Requirements

1. Mandatory Due Diligence for AePS Touchpoint Operators (ATOs)

Acquiring banks, defined as banks that onboard AePS touchpoint operators must now:

- Conduct full Know Your Customer (KYC) verification and due diligence of AePS Touchpoint Operators (ATOs) as per the RBI's KYC Master Directions, which lay down the procedure for verifying identity and address of individuals before onboarding.
- If the ATO is already onboarded as a Business Correspondent (BC) or sub-agent, the bank may rely on existing KYC, subject to verification.
- Undertake periodic KYC updation for all ATOs.

Importantly, ATOs who remain inactive for three continuous months (i.e., perform no financial or non-financial transactions) must undergo KYC again before being reactivated.

2. Operational and Risk Controls

Banks are directed to:

- Monitor ATOs through transaction surveillance systems;
- Define risk-based operational parameters, such as limits based on geography, volume, or transaction type;
- Continuously review these parameters to reflect emerging fraud trends;
- Ensure API integrations or system-level technologies are only used for bona fide AePS operations and not for ancillary or unregulated services.

This significantly elevates the oversight burden on acquiring banks and aligns fraud risk controls for AePS with core banking channels.

Regulatory Implications

This directive marks a significant compliance enhancement for AePS channel governance. Its implications are far-reaching:

- **For Banks:** There will be a need to revisit existing contracts, audit trails, and KYC documentation of all AePS agents, particularly those onboarded through BC networks. Banks must also build or upgrade real-time monitoring systems to track ATO-level risks.
- **For Fintechs and White-Label AePS Integrators:** Entities partnering with banks to extend AePS services must align their onboarding, training, and transaction monitoring modules with the RBI framework. API misuse or absence of fraud detection flags may expose partner entities to indirect liability.
- **For Regulatory Compliance Officers:** The dual reliance on PSS Act and KYC Master Directions mandates internal legal teams to ensure that these obligations are integrated into bank-wide compliance workflows, including those for Business Correspondents.
- **For Financial Inclusion Stakeholders:** While these steps may increase onboarding friction at the grassroots level, they also serve to prevent identity theft and unauthorised withdrawals — key deterrents in low-literacy banking ecosystems.

Context and Industry Backdrop

AePS transactions which facilitate interoperable banking services using Aadhaar number and biometric or OTP authentication have surged in volume, especially in DBT disbursal and cash withdrawal services. However, the same accessibility has exposed rural users to identity spoofing, cloned biometrics, and unauthorised withdrawals, resulting in regulatory concern.

In the RBI's Statement on Developmental and Regulatory Policies dated 8th February 2024, it had already flagged AePS-related vulnerabilities and expressed intent to strengthen touchpoint governance. This June 2025 directive operationalises that policy intent.

Conclusion

The RBI's 27th June 2025 directions for due diligence and fraud risk management of AePS touchpoint operators represent a significant shift in how last-mile banking infrastructure will be regulated in India. It places legal and operational responsibility squarely on acquiring banks to ensure that AePS agents are not just accessible but also accountable.

The regulatory emphasis on KYC parity, transaction risk analysis, and system integrity is a timely response to the scale of Aadhaar-based financial delivery. With the compliance deadline of 1st January

2026, institutions must begin immediate review of their AePS frameworks, agent due diligence standards, and fraud surveillance controls to meet the mandate.

For more details, write to us at: contact@indialaw.in

Related Practice Areas

Banking & Finance