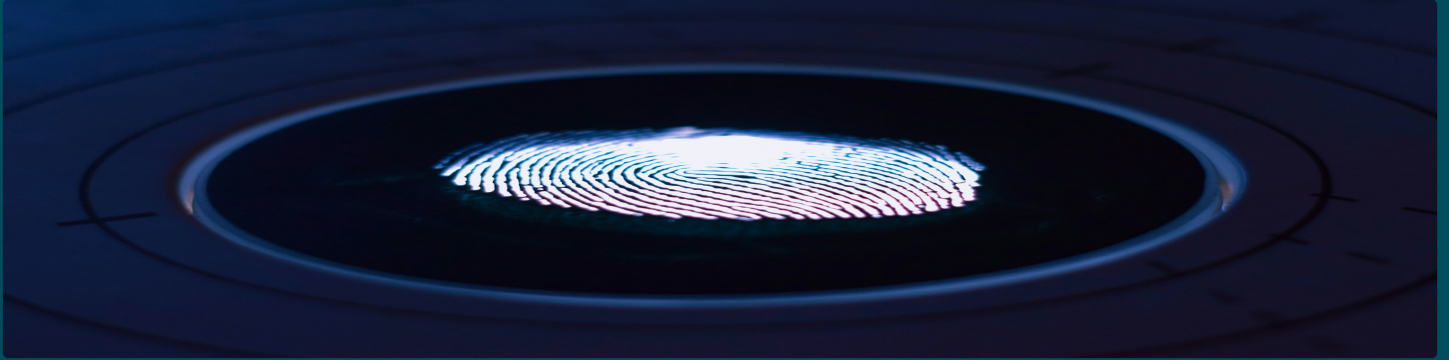




REGULATORY

Aadhaar Authentication and Offline Verification Amendment Regulations, 2025: Strengthening India's Digital Identity Framework

AUTHOR Ayush Shukla

PUBLISHED 16 December 2025

Introduction

The Unique Identification Authority of India (UIDAI) has notified the Aadhaar Authentication and Offline Verification Amendment Regulations, 2025. Issued under Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the amendment revises and expands the Aadhaar Authentication and Offline Verification Regulations, 2021. The update modernises the technological framework of Aadhaar-based offline verification and deepens compliance mechanisms, strengthens user protection, and introduces an advanced set of digital verification tools. Collectively, these amendments highlight India's commitment to secure, flexible, and privacy-respecting identity verification in an increasingly digitised economy.

Table of contents

- [Introduction](#)
- [Factual Background](#)
- [New Definitions and Technological Concepts Introduced](#)
- [Revised Framework for Types of Offline Verification](#)
- [Registration of Offline Verification Seeking Entities \(OVSEs\)](#)
- [Surrender, Closure, and Record-Retention Obligations](#)
- [Amendments to Penalties, Compliance, and Enforcement](#)
- [Technological Advancements Reflected in the Amendment](#)
- [Legal Significance and Compliance Impact](#)
- [Conclusion](#)

Factual Background

Offline Aadhaar verification, unlike online authentication, enables identity verification without a live connection to UIDAI's Central Identities Data Repository (CIDR). This mechanism is critical for last-mile verification, low-connectivity environments, privacy-preserving KYC, and reducing dependency on live authentication channels. The 2025 amendment is introduced against the backdrop of increasing reliance on digital financial services, e-governance portals, and secure identity credentials, especially for fintech, banking, telecom, education, travel and other service sectors. The amendments aim to broaden the ecosystem by allowing more entities to use offline verification while ensuring accountability and strong regulatory oversight.

New Definitions and Technological Concepts Introduced

A substantial component of the amendment lies in the insertion of advanced terminology into Regulation 2. The introduction of the term "Aadhaar Application" brings multiple UIDAI-managed digital platforms such as Aadhaar App, mAadhaar, myAadhaar Portal, Aadhaar QR Scanner under a unified regulatory umbrella, ensuring seamless and standardised service delivery.

An addition is the "Aadhaar Verifiable Credential" (AVC). This digitally signed, user-controlled credential contains limited demographic data and is cryptographically verifiable. It enables selective disclosure of information, aligning India's digital identity system with global standards of verifiable credentials and self-sovereign identity (SSI). AVCs mark a technological leap in privacy protection and decentralised identity verification.

The amendment also introduces "Offline Face Verification", wherein a live facial capture is matched locally against the photograph embedded within an Aadhaar application. This eliminates the necessity for CIDR-based authentication while maintaining verification accuracy, representing a major advancement in biometric offline authentication.

Revised Framework for Types of Offline Verification

Regulation 3A has been entirely substituted to redefine the offline verification ecosystem. It now recognises multiple digital and document-based modes, including QR code-based verification, e-Aadhaar verification, paperless offline e-KYC, Aadhaar Verifiable Credential verification, and future modes to be notified. Crucially, UIDAI has permitted offline verification with or without offline face verification, depending on technological specifications. By expanding the permissible modes, the amendment ensures adaptability, scalability, and alignment with evolving digital identity technologies.

UIDAI will also provide mechanisms for downloading QR codes, e-Aadhaar, AVCs, or paperless e-KYC packages through the Aadhaar application, ensuring secure distribution channels controlled by the authority.

Registration of Offline Verification Seeking Entities (OVSEs)

A pivotal regulatory development is the creation of Regulation 13A, which introduces a full-fledged, formalised registration framework for Offline Verification Seeking Entities (OVSEs). Any entity wishing to use Aadhaar paperless offline e-KYC or Aadhaar Verifiable Credentials through Aadhaar applications must undergo UIDAI scrutiny, meet eligibility norms, and demonstrate lawful purpose.

UIDAI now possesses powers to seek clarifications, inspect submitted information, approve or reject applications, and impose fees for registration and per-verification transactions. Rejected applicants receive written reasons and a statutory right of reconsideration within 30 days. This ensures due process, transparency, and graded regulatory control over both public and private sector entities.

Surrender, Closure, and Record-Retention Obligations

The insertion of Regulation 23A governs the surrender of access by OVSEs. An entity may voluntarily exit, but UIDAI mandates stringent closure procedures to ensure data continuity and user rights. OVSEs must maintain and preserve verification logs, address grievance records, provide access to verification details sought by Aadhaar holders, and settle financial accounts with UIDAI. This approach prevents abrupt termination, ensuring a smooth regulatory off-boarding process and safeguarding privacy and record integrity.

Amendments to Penalties, Compliance, and Enforcement

The amendment strengthens UIDAI's enforcement capacity through changes to Regulations 251A, 252 and 253. The revised penalty framework extends liability to Requesting Entities, Sub-AUAs, Sub-KUAs, and OVSEs. UIDAI may impose penalties for non-compliance, unlawful use, failure to provide information, and non-cooperation during audits or investigations. Before action is taken, the entity is afforded a reasonable opportunity to be heard, ensuring procedural fairness.

Regulation 253 now requires entities whose appointment or registration is terminated to cease use of the Aadhaar name and logo and to prove completion of closure steps, including those under the new surrender provisions. The removal of references to outdated formats such as XML and m-Aadhaar reflects technological modernisation and transition to newer, more secure formats.

Technological Advancements Reflected in the Amendment

This regulatory update reflects multiple technological advancements in India's identity ecosystem:

- **Introduction of Verifiable Credentials (AVCs):** A major leap aligned with global Web 3.0 identity models, enabling selective disclosure and cryptographic proofing.
- **Offline Facial Biometrics:** Brings secure biometric verification to remote environments without reliance on UIDAI servers.
- **Unified Aadhaar Application Ecosystem:** Standardises service delivery across all UIDAI-run digital platforms.
- **Enhanced Data Portability and User Control:** Through paperless offline e-KYC and downloadable credentials.
- **Modernisation of file formats and verification modes:** Moving away from legacy XML formats to more secure, contemporary formats.
- **Scalable Verifications for high-volume entities:** Allowing government, fintechs, NBFCs, telecom operators, and digital service platforms to adopt Aadhaar-based verification without overloading authentication networks.

Legal Significance and Compliance Impact

This marks a substantial strengthening of UIDAI's supervisory powers and accountability norms for verification entities. Registration, monitoring, suspension, and penalty mechanisms are now explicitly codified. The introduction of AVCs creates a privacy-protective alternative to earlier e-KYC flows, reducing exposure of full Aadhaar numbers and demographic data. The mandatory preservation of logs and record-access rights enhances transparency for Aadhaar holders, and stronger penalties provide deterrence against misuse.

The amendment also directly aligns with data protection principles under the Digital Personal Data Protection Act, 2023, particularly concerning purpose limitation, storage limitation, user access rights, and lawful processing.

Conclusion

The Aadhaar Authentication and Offline Verification Amendment Regulations, 2025 represent a forward-looking recalibration of India's digital identity infrastructure. By combining legal safeguards with technological sophistication such as verifiable credentials, offline biometrics, and expanded offline verification modes, the amendment encourages a secure, inclusive, and privacy-centric verification environment. The framework will benefit regulated sectors, support digital public infrastructure, and enhance trust in Aadhaar-based services, while ensuring that entities using these facilities remain accountable, compliant, and transparent.

For further details write to contact@indialaw.in

Related Practice Areas

Statutory And Regulatory Compliance