WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Impact of Digital Identity Verification on NBFC Compliance under the Prevention of Money Laundering Act, 2002

Siddharth Krishnan[1], Dr. Ranjana Sharma[2]

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

Digital identity verification has become the keystone of NBFC compliance under India's Prevention of Money Laundering Act, 2002, reshaping onboarding, monitoring, record-keeping, and reporting. This study examines the impact of digital identity verification on Non-Banking Financial Companies' compliance under the "Prevention of Money-laundering Act, 2002" in India, focusing on onboarding, monitoring, record-keeping, and reporting. It pursues a doctrinal analysis of the "Prevention of Money-laundering (Maintenance of Records) Rules, 2005" as amended through 2023, the "Master Direction - Know Your Customer (KYC) Direction, 2016" with Video-based Customer Identification Process (V-CIP) introduced on January 9, 2020 and updated through 2023–2025, UIDAI's "Aadhaar (Authentication and Offline Verification) Regulations, 2021", and the "Digital Personal Data Protection Act, 2023". The study maps how Aadhaar online e-KYC, Aadhaar paperless offline e-KYC, V-CIP, CKYCR pulls using the KYC Identifier, and acceptance of equivalent e-documents such as DigiLocker and e-PAN reduce turnaround time, improve audit trails, and expand remote onboarding while carrying novel risks such as deepfakes and synthetic identities. It shows that 2023 PML Rules lowered beneficial ownership thresholds to 10 percent in companies and partnerships, tightening NBFC obligations for beneficial owner discovery, while RBI's V-CIP safeguards require liveness, geo-tagging, officer-led capture, and prohibit printed e-documents to raise assurance. It integrates DPDP Act duties on consent, breach intimation, retention, and significant data fiduciary governance with PMLA's ten-year record norms, clarifying how lawful retention under anti-money laundering legislation coexists with data minimisation and erasure triggers. Finally, it reads FATF Digital ID guidance on assurance levels and remote onboarding as a benchmark for risk-based controls in Indian NBFC practice, arguing that digital identity modalities now sit at the core of an NBFC's PMLA compliance architecture, provided consent, auditability, and continuous monitoring are embedded by design.[1]

Keywords: PMLA; NBFC; e-KYC; V-CIP; Aadhaar; CKYCR; FIU-IND; DPDP Act; Beneficial ownership; FATF

Introduction

Non-Banking Financial Companies operate at scale across retail credit, asset finance, housing finance, and fintech partnerships, and are designated "reporting entities" under the anti-money laundering framework. Under "Section 12 of the Prevention of Money-laundering Act, 2002" and the "Prevention of Money-laundering (Maintenance of Records) Rules, 2005", NBFCs must collect and verify client identity and beneficial ownership information, maintain records, apply a risk-based approach to customer due diligence, and furnish prescribed reports to FIU-IND. Digital identity verification has reshaped these duties. Aadhaar e-KYC, Aadhaar paperless offline e-KYC, V-CIP, CKYCR retrievals using the KYC Identifier, and acceptance of equivalent e-documents such as DigiLocker and e-PAN have transformed onboarding from branch-heavy workflows to remote, auditable streams.[2] This transformation is not merely operational. It flows from a layered legal architecture that spans "Section 11A of the Prevention of Money-laundering Act, 2002" on Aadhaar authentication by notified entities, the RBI's "Master Direction - KYC Direction, 2016" with its 2020 V-CIP insertion and subsequent amendments through 2023, UIDAI's 2021 Regulations on authentication and offline verification, 2023 PML Rules amendments tightening beneficial ownership and group-wide norms, and the "Digital Personal Data Protection Act, 2023" which codifies consent, breach intimation, security safeguards, and retention aligned to statutory mandates.[3]

The regulatory pivots are concrete. RBI introduced V-CIP on January 9, 2020 with detailed safeguards around officer-led live video, liveness, clear PAN capture or e-PAN verification, geo-tagging to ensure the customer's presence in India, and a ban on printed copies of equivalent e-documents during video KYC.[4] RBI has continued to update the Master Direction and FAQs through 2023–2025 to clarify acceptance of CKYCR records via the KYC

[1] Master Direction – Know Your Customer (KYC) Direction, 2016, *available at:* https://www.rbi.org.in/commonman/English/scripts/notification.aspx?id=2607 (last visited on November 3, 2025).
[2] Vidushi Marda, Amber Sinha, "FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy", 18 *Indian Journal of Law and Technology* 72 (2022).
[3] The Prevention of Money-Laundering Act, 2002, *available at:* https://enforcementdirectorate.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf (last visited on November 2, 2025).
[4] Shankkar Aiyar, *Aadhaar: A Biometric History of India's 12-Digit Revolution* 164 (Westland, Chennai, 1st edn., 2017).

Identifier with explicit consent, the use of equivalent e-documents including DigiLocker, and re-KYC via V-CIP. In March–September 2023, amendments to the PML Rules lowered beneficial ownership thresholds for companies and partnerships to more than 10 percent and added clarity for trusts and unincorporated bodies, heightening NBFC duties to identify natural-person controllers. Parallelly, UIDAI's 2021 Regulations codified both Aadhaar authentication and offline verification pathways, mirroring the Aadhaar and Other Laws Amendment's emphasis on voluntary use and offline modes.[5] These changes have embedded digital identity at the centre of NBFC AML compliance, yet they also demand stronger model governance against impersonation, deepfakes, and synthetic identities, and tighter alignment between PMLA's ten-year record requirements and DPDP Act erasure demands subject to legal retention.[6]

Research Questions

The research questions for the study are as follows:-[7]

1. whether digital KYC modalities improve compliance efficacy and risk outcomes for NBFCs under "Sections 11A, 12, and 12AA of the PMLA" while maintaining proportionality and accuracy?
2. whether the combined use of V-CIP, Aadhaar offline e-KYC, CKYCR retrievals, and equivalent e-documents yields stronger onboarding assurance and better FIU-IND reporting performance compared to traditional face-to-face methods?

Problem Statement

NBFCs rely on Aadhaar e-KYC where permitted under "Section 11A notifications", Aadhaar paperless offline e-KYC, CKYCR pulls using a KYC Identifier, and V-CIP to scale remote onboarding. Emerging fraud vectors such as deepfakes and synthetic identities challenge these processes, creating a compliance-risk tension between speed and assurance. 2023 PML Rules changes lowered beneficial owner thresholds to more than 10 percent, intensifying identification burdens, while DPDP Act duties on consent, security, and breach intimation overlay KYC data handling. The problem is how NBFCs reconcile these overlapping mandates while maintaining audit-quality trails, preserving privacy, and ensuring reliable risk classification across digital channels.[8]

Objectives of the Study

The objectives of the study are as follows:-[9]

1. To analyse how Aadhaar online e-KYC, Aadhaar paperless offline e-KYC, V-CIP, CKYCR retrievals, and equivalent e-documents shape NBFC compliance under the "PMLA" and "PML Rules".
2. To evaluate how DPDP Act duties on consent, breach intimation, and retention interact with PMLA's record-keeping and FIU-IND reporting obligations across digital KYC workflows.

Research Methodology

The study adopts a doctrinal methodology anchored in the text of the "PMLA", the "Prevention of Money-laundering (Maintenance of Records) Rules, 2005" as amended in 2023, RBI's "Master Direction - KYC Direction, 2016" and related circulars and FAQs, UIDAI's "Aadhaar (Authentication and Offline Verification) Regulations, 2021", FIU-IND guidance on reporting formats and roles, and the "Digital Personal Data Protection Act, 2023". Practitioner circulars are read to the extent they reflect binding direction. Brief practitioner interviews are considered optional context. The analysis relies on official gazettes, regulator sites, and authoritative bodies including FATF for normative benchmarks on digital identity assurance.[10]

Regulatory Framework

NBFC KYC and AML duties emerge from a hierarchy of binding sources. The "PMLA" sets the core obligations on record-keeping, client verification, and information furnishing, with "Section 11A" codifying verification channels, "Section 12" prescribing record-keeping and identity verification, and "Section 12AA" providing for enhanced due diligence on specified transactions or in higher-risk contexts. The "PML Rules" operationalise procedures, define central concepts including client due diligence and suspicious transactions, and create the Central KYC Records Registry architecture with Rule 9 and Rule 9A setting procedures for CKYCR submissions, retrievals, and updates. RBI's "Master Direction - KYC Direction, 2016" applies to NBFCs as regulated entities and supplies detailed processes such as V-CIP, digital KYC, acceptance of equivalent e-documents including DigiLocker, and periodic

[5] Taxmann Editorial Board, *Money Laundering Law Manual* 132 (Taxmann Publications, New Delhi, 1st edn., 2023).
[6] Amendment to Master Direction on KYC, *available at:* https://img1.digitallocker.gov.in/circulars/RBI_master_circular_on_eKYC_09.01.2020.PDF (last visited on November 1, 2025).
[7] Vrinda Bhandari, Renuka Sane, "A Critique of Aadhaar Framework", 31 *National Law School of India Review* 58 (2019).
[8] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), s. 11A.
[9] Nupur Chowdhury, "Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy", 11 *NUJS Law Review* 96 (2018).
[10] Indian Institute of Banking & Finance, *Non-Banking Financial Companies* 176 (Taxmann Publications, New Delhi, 1st edn., 2025).

updation. UIDAI's 2021 Regulations define both authentication and offline verification, aligned with the Aadhaar and Other Laws Amendment that underscores voluntary use and offline modes, while the DPDP Act overlays duties to ensure lawful processing, security safeguards, breach intimation to the Board and affected data principals, and retention limited to legal necessity. FATF's 2020 Digital ID Guidance supplies assurance-level benchmarks and risk-based expectations for non-face-to-face onboarding.[11]

PMLA and PML Rules

The PMLA's Chapter IV binds NBFCs as "reporting entities" with duties to maintain transaction records and verify client identities. "Section 12" requires recording prescribed transactions and identity data, with a ten-year retention period from the date of cessation of the client relationship, and the "PML Rules" reinforce ten-year retention for records under Rule 3. "Section 11A" sets identity verification routes, allowing Aadhaar authentication for entities notified by the Central Government, and "Section 12AA" stipulates enhanced due diligence where specified transactions or higher-risk indicators exist. The "PML Rules, 2005" as amended through March and September 2023 refine customer due diligence, define or update terms such as digital KYC and equivalent e-documents, and, critically, lower beneficial ownership thresholds to more than 10 percent for companies and partnerships while specifying identification of trust parties and unincorporated associations. Rule 9A and allied clauses establish the functions and obligations of the Central KYC Records Registry and mandate real-time access with explicit conditions for retrieval using the KYC Identifier, and limited re-collection of documents unless the downloaded record is incomplete, outdated, or otherwise requires update. These prescriptive texts anchor NBFC obligations that are then elaborated in RBI's domain-specific directions.[12]

RBI KYC Directions for Regulated Entities

RBI's "Master Direction - KYC Direction, 2016" applies across banks and NBFCs, requiring risk-based customer due diligence and specifying modalities for face-to-face and non-face-to-face onboarding. On January 9, 2020, RBI inserted V-CIP as an alternate method where an authorised officer conducts a live, consented audio-visual interaction, captures the customer's photograph, and verifies PAN or e-PAN with the issuing authority. The Direction and subsequent clarifications require geo-tagging with live GPS coordinates, date-time stamping, and concurrency checks, and disallow printed copies of equivalent e-documents during V-CIP to pre-empt tampering. Updates across 2023–2025 reiterate acceptance of KYC records downloaded from CKYCR using the KYC Identifier with explicit customer consent, acceptance of equivalent e-documents including DigiLocker, and the permissibility of re-KYC via V-CIP, tightening controls for non-face-to-face onboarding. Together with periodic updation norms and risk segmentation, these prescriptions embed technology with auditability and chain-of-custody safeguards.[13]

Aadhaar Legal Architecture

Aadhaar's legal framework now emphasises voluntary use and allows offline verification modalities. The "Aadhaar and Other Laws (Amendment) Act, 2019" clarifies that an Aadhaar number holder may voluntarily use Aadhaar in physical or electronic form by authentication or offline verification. UIDAI's "Aadhaar (Authentication and Offline Verification) Regulations, 2021" detail yes/no and e-KYC authentication routes, as well as offline verification via QR codes or digitally signed XML, and codify the manner of voluntary use including paperless mechanisms and mAadhaar. "Section 11A of the PMLA" permits reporting entities notified by the Central Government to use Aadhaar authentication for client and beneficial owner verification; notifications in recent years have specified lists of entities, including NBFCs, that may perform authentication for PMLA purposes. This enables NBFCs to adopt Aadhaar online e-KYC under a lawful basis, while enabling Aadhaar offline e-KYC for entities that are not so notified, preserving consent as the cornerstone.[14]

Data Protection Overlay

The "Digital Personal Data Protection Act, 2023" overlays KYC activities with clear duties. "Section 8" sets general obligations, including implementing appropriate technical and organisational measures, security safeguards to prevent personal data breaches, and intimation of a personal data breach to the Board and each affected data principal in the prescribed manner. "Section 8(7)" requires erasure when consent is withdrawn or the purpose is no longer served, except where retention is necessary to comply with law. An illustration explicitly states that a bank may retain identity records for ten years after account closure where another law requires it, aligning with PMLA retention. The Act mandates transparent notices, lawful bases including consent, publication of contact information of the Data Protection Officer for significant data fiduciaries, and grievance redressal mechanisms. For NBFCs handling large-scale KYC data, this framework anchors privacy-by-design without displacing "PMLA" obligations that necessitate long-lived identity and transaction records for audits and FIU-IND reporting.[15]

International Standards

FATF's "Guidance on Digital Identity" positions digital ID as compatible with standard or even low-risk non-face-to-face onboarding when appropriate assurance levels are achieved. It encourages authorities to clarify acceptance of digital ID and instructs regulated entities to adopt risk-based approaches to reliance on digital ID systems, focusing on performance and outcomes such as error rates, spoof resistance, and portfolio risk. India's 2023 FATF

---

[11] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 208 (HarperCollins, New Delhi, 1st edn., 2018).
[12] Kharak Singh v. State of Uttar Pradesh, *available at:* https://indiankanoon.org/doc/290623/ (last visited on October 30, 2025).
[13] Commercial Law Publishers Editorial Team, *Commentary on the Prevention of Money Laundering Act, 2002* 145 (Commercial Law Publishers, New Delhi, 1st edn., 2024).
[14] The Aadhaar and Other Laws (Amendment) Act, 2019, *available at:* https://uidai.gov.in/images/news/Amendment_Act_2019.pdf (last visited on October 29, 2025).
[15] Indian Institute of Corporate Affairs Faculty, *Data Protection and Financial Services in India* 189 (OakBridge, New Delhi, 1st edn., 2021).

Mutual Evaluation indicates active alignment with the FATF 40 Recommendations and evidences recent improvements in AML/CFT measures, setting expectations for supervisory attention to remote onboarding controls. For NBFCs, the FATF baseline helps interpret RBI's V-CIP prescriptions and UIDAI assurance mechanisms through a recognisable lens of assurance levels and governance.[16]

Digital Identity Modalities in Nbfc Onboarding

Digital identity modalities form a toolkit that can be mixed according to regulatory permissions, risk tier, and channel. Aadhaar online e-KYC via authentication under "Section 11A notifications" offers near-real-time identity confirmation where permitted, with demographic and photograph attributes sourced from UIDAI. Aadhaar paperless offline e-KYC uses digitally signed XML or secure QR without contacting UIDAI during verification, useful where the entity lacks Aadhaar authentication permission. V-CIP creates an officer-led, geo-tagged, recorded interaction that integrates OVD or Aadhaar elements and tightens non-face-to-face controls against spoofing. CKYCR retrievals using a KYC Identifier reduce duplication and enable rapid onboarding if the record is complete and current; explicit consent is required for pulls. Acceptance of equivalent e-documents including those issued through DigiLocker and e-PAN extends reliability while lowering friction. Each modality has different assurance and consent contours that must be mapped to risk-based policies.[17]

Aadhaar Online E-KYC and Authentication

Aadhaar online e-KYC is available to entities notified under the first proviso to "Section 11A(1) of the PMLA". For such notified NBFCs, Aadhaar authentication supports identity verification of clients and beneficial owners, subject to explicit consent, purpose limitation, and UIDAI security and privacy standards. The process provides demographic data and photograph from UIDAI, improving assurance when combined with risk-based controls. Non-notified NBFCs cannot perform Aadhaar authentication but can still rely on Aadhaar in offline modes. Auditable consent records are essential because UIDAI and RBI both stress the primacy of consent for e-KYC and CKYCR pulls. RBI's KYC framework acknowledges Aadhaar OTP e-KYC and biometric e-KYC where applicable, but requires masking of Aadhaar numbers in internal records and restricts reuse beyond lawful purposes. The compliance advantage lies in speed and verifiable source data; the risk lies in over-collection or misuse without proper consent logging and retention bounds under the DPDP Act.[18]

Aadhaar Paperless Offline E-KYC

Aadhaar paperless offline e-KYC operates without network authentication to UIDAI at the time of verification. It relies on digitally signed XML or secure QR codes generated by the Aadhaar holder, whose integrity can be verified using UIDAI's public keys. UIDAI's 2021 Regulations codify the manner of voluntary offline use, including acceptance of Aadhaar letter, PVC card, e-Aadhaar, and XML packages, which Offline Verification Seeking Entities must validate. RBI links offline Aadhaar to V-CIP with a freshness requirement: when used during V-CIP, the XML or secure QR generation date must not be older than three days, strengthening anti-spoofing measures. For NF2F onboarding by NBFCs lacking Aadhaar authentication permission, offline e-KYC provides a high-quality signal while preserving the voluntary design of Aadhaar use, contingent on auditable consent and appropriate masking of Aadhaar numbers in internal records.[19]

Video-based Customer Identification Process

V-CIP functions as a high-assurance alternative to in-person interaction, tailored for remote onboarding and re-KYC. It requires an authorised officer to conduct a live, consented audio-visual session, record audio-video, capture a clear customer photograph, verify PAN or e-PAN against the issuing authority, and ensure that photographs on the OVD or Aadhaar match the customer on video. RBI requires live geo-tagging to confirm presence within India, date-time stamping, and controls against IP spoofing. It prohibits the use of printed copies of equivalent e-documents such as e-PAN during V-CIP, insisting on direct digital verification. RBI's workflow requirements include concurrency checks and concurrent audit before operationalising V-CIP accounts, raising assurance and evidentiary value. These features collectively provide a multi-layered defense against deepfakes and replay attacks while preserving a complete audit trail, which aligns with both FIU reporting expectations and DPDP security safeguards.[20]

Ckycr Pulls and KYC Identifier Use

CKYCR reduces friction by allowing NBFCs to retrieve a customer's KYC record in real time using the KYC Identifier, subject to explicit consent. The "PML Rules" require reporting entities to upload KYC records to CKYCR within ten days of commencing an account-based relationship and to keep them updated. When a KYC Identifier exists, the reporting entity must pull the record and should not re-collect documents unless the downloaded record is incomplete, outdated, or its validity period has lapsed, or where additional verification is necessary for address, enhanced due diligence, or risk profiling.

---

[16] Guidance on Digital Identity, *available at:* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf (last visited on October 28, 2025).

[17] Somesh Arora, *Prevention of Money Laundering Act, 2002: A Commentary* 154 (OakBridge, New Delhi, 1st edn., 2023).

[18] Renuka Thapar, "e-KYC and Financial Inclusion: Regulatory Design for Trust and Risk", 9 *NLSIU National Law School Journal* 88 (2019).

[19] The Aadhaar (Authentication and Offline Verification) Regulations, 2021, *available at:* https://uidai.gov.in/images/The_Aadhaar_Authentication_and_Offline_Verifications_Regulations_2021.pdf (last visited on October 27, 2025).

[20] Rajat Bhatia, Video KYC, *V-CIP and Digital Onboarding: Legal Standards and Controls* 172 (Bloomsbury Professional India, New Delhi, 1st edn., 2021).

CKYCR must provide real-time access and notify reporting entities of updates, which entities are then obliged to reflect in their own records. RBI's FAQs further emphasise the need for explicit consent before download, reinforcing the consent-centric structure around shared KYC infrastructure.[21]

Digilocker and Equivalent E-Documents

Equivalent e-documents, including those issued through DigiLocker and e-PAN, are recognised for customer due diligence under RBI's KYC Directions. The concept of "equivalent e-document" captures an electronic equivalent issued with a valid digital signature by the issuing authority, which includes documents in a customer's DigiLocker account. RBI's 2020 V-CIP circular and the Master Direction reiterate acceptance of such e-documents, while prohibiting printed copies during V-CIP to prevent tampering. For NBFCs, DigiLocker reduces collection friction and streamlines verification with strong provenance, especially when combined with CKYCR pulls and V-CIP. This reduces onboarding time without compromising auditability, provided that consent capture, masking of Aadhaar numbers, and secure storage are enforced with DPDP-consistent controls.[22]

Modality	**Regulatory basis**	**Assurance level**	**Fraud risks**	**Audit trail**	**Turnaround time**	**Cost**
Traditional face-to-face KYC	"PMLA" and "PML Rules"; RBI KYC Directions OVD norms	High when OVD authenticity is verified; physical presence	Document forgery; impersonation at branch	Paper plus system logs; weaker media evidence	Slow due to physical visits	Higher per-customer handling
Aadhaar paperless offline e-KYC	"UIDAI 2021 Regulations" on offline verification; RBI KYC linking to V-CIP freshness	High when XML/QR signature verified; no network call	Synthetic identities if not cross-checked; replay if stale	Cryptographic artefacts and verification logs	Fast when customer provides XML/QR	Low once integrated
Aadhaar online e-KYC	"Section 11A of PMLA" notifications; UIDAI authentication	Very high for notified entities using UIDAI e-KYC	Over-reliance without consent logs; ecosystem misuse	Strong source logs plus internal consent records	Near-real-time	Low to moderate per transaction
V-CIP	RBI KYC Direction V-CIP clauses and 2020 circular	High with liveness, geo-tagging, officer-led checks	Deepfakes and spoofing if controls weak	Full audio-video, geo-tags, timestamps	Fast once scheduled	Moderate due to staffing and audit

Table 1: Comparative features across key identity verification modalities relevant to NBFC onboarding in India, mapped to regulation, assurance, risk, evidentiary trail, speed, and cost.

Nbfc Compliance Duties under PMLA

NBFCs must translate digital identity tools into compliant workflows across due diligence, beneficial ownership discovery, ongoing monitoring, record-keeping, and FIU-IND reporting. "Section 12" codifies record-keeping and identity verification with a ten-year retention, while "Section 11A" and the "PML Rules" define acceptable verification methods. "Section 12AA" introduces enhanced due diligence for specified transactions and higher-risk situations. RBI's KYC Direction sets the operational detail for risk-based CDD, V-CIP, periodic updation, and acceptance of CKYCR and equivalent e-documents. FIU-IND guidance fixes timelines for Cash Transaction Reports (CTR) by the 15th of the succeeding month and Suspicious Transaction Reports (STR) within seven working days of arriving at suspicion, while requiring designation of a Designated Director and a Principal Officer. The question is how digital identity reduces false onboarding, improves beneficial owner discovery after the 2023 thresholds, and strengthens monitoring without triggering privacy non-compliance. The answer lies in consent architecture, tamper-evident audit trails, and event-driven updates anchored by CKYCR and V-CIP.[23]

Customer Due Diligence and Ovds

Customer Due Diligence rests on verifying identity and address using OVDs or equivalent e-documents, Aadhaar authentication where notified, offline verification, CKYCR downloads via KYC Identifier, and V-CIP. RBI's framework allows non-face-to-face onboarding provided the RE adheres to V-CIP controls and ensures consent-based retrievals from CKYCR. OVD options extend through DigiLocker when the issuing authority's digital signature is intact. For reliance on third-party records such as CKYCR, the "PML Rules" circumscribe re-collection: an NBFC must rely on downloaded KYC records unless the record is incomplete or non-compliant with current norms, or verification of current address or enhanced due diligence is necessary. Digital KYC under the PML Rules uses live photograph capture linked with OVD or proof of possession of Aadhaar, reflecting the system's move toward

[21] PML (Maintenance of Records) Rules, 2005, *available at:* https://fiuindia.gov.in/files/AML_Legislation/notification.html (last visited on October 26, 2025).
[22] Reserve Bank Compliance Forum, KYC, *CKYCR & Digital Identity for REs* 205 (Taxmann Publications, New Delhi, 1st edn., 2022).
[23] Dr. Shamsuddin, *Commentary on the Prevention of Money Laundering Act, 2002* 233 (Commercial Law Publishers, New Delhi, 1st edn., 2024).

multimedia evidence. These blended options should be used to align assurance with customer risk, and to build auditable trails needed for FIU-IND investigations and supervisory inspections.[24]

Beneficial Ownership and Edd

Beneficial ownership thresholds were tightened in 2023. The RBI KYC Direction now recognises that, for companies, controlling ownership interests of more than 10 percent trigger beneficial owner identification; for partnerships, ownership or entitlement to more than 10 percent of capital or profits, or control through other means, similarly triggers identification. Trusts require identifying the author, trustees, beneficiaries with 10 percent or more interest, and any natural person exercising ultimate effective control. This lowering from earlier 15 or 25 percent standards contracts the anonymity space and places higher onus on NBFCs to map ownership chains and control rights. Enhanced due diligence under "Section 12AA" and RBI's risk guidance must be applied to high-risk entities and PEP-linked customers, with portfolio-level screening against FATF statements and public information to detect higher-risk jurisdictions or exposure. The move to 10 percent in companies and partnerships makes CKYCR updates, document provenance, and board or partnership deed verification essential, especially when onboarding is digital and non-face-to-face.[25]

Ongoing Monitoring and Periodic Updation

The duty to know the customer persists beyond onboarding. RBI's KYC Direction requires ongoing monitoring and periodic updation calibrated to risk category, with re-KYC permissible through V-CIP under defined conditions. Event-based updates include changes in address, beneficial ownership, or control, and CKYCR notifications of updated records must be mirrored in the NBFC's systems. Digital identity supports monitoring by enabling event-driven reviews and simplified re-verification without branch visits, provided that explicit consent is recorded for CKYCR pulls and that updated e-documents are obtained in equivalent form with digital signatures. V-CIP's recorded sessions, time-stamps, and geo-tags create strong evidence of continued customer contact and enable comparison checks with prior media to detect anomalies. DPDP Act requirements on accuracy and security reinforce the case for structured re-KYC cadences and automated prompts tied to document validity and risk changes.[26]

Record-keeping and Data Retention

PMLA and the PML Rules mandate ten-year retention. "Section 12(2)" requires maintaining transaction records for ten years from the date of the transactions, and identity records for ten years from the date of cessation of the relationship, while Rule 6 of the PML Rules sets a ten-year minimum for records referred to in Rule 3. These legal duties co-exist with the DPDP Act's erasure principle, which is expressly qualified by lawful retention; an illustration in "Section 8" confirms that a bank may retain identity records for ten years post-closure where law requires. For NBFCs, digital identity artefacts such as V-CIP recordings, Aadhaar offline XML signatures, CKYCR pull logs, and DigiLocker document hashes must be stored with integrity controls, access governance, and well-documented retention schedules. This reconciles auditability with privacy by confining retention and processing to statutory compliance, and by instituting breach response protocols that include timely intimation to the Board and affected data principals as per the DPDP Act.[27]

Fiu-ind Reporting

NBFCs must furnish FIU-IND reports in prescribed formats and timelines. Cash Transaction Reports are due by the 15th of the succeeding month, while Suspicious Transaction Reports must be filed within seven working days of arriving at a conclusion of suspicion. Reporting regimes also include Non-profit Organisation Transaction Reports and Cross-Border Wire Transfer Reports as specified. The "PML Rules" and FIU-IND guidance require each reporting entity to designate a Designated Director responsible for overall compliance and a Principal Officer responsible for reporting to FIU-IND, with contact details to be communicated promptly upon appointment. Digital identity processes enhance the quality of FIU-IND submissions by improving attribute accuracy, providing time-stamped and geo-tagged evidence in V-CIP logs, and enabling faster risk escalation from onboarding to investigation. The legal architecture here works best when digital KYC artefacts and consent logs are retrievable and linked to monitoring alerts, allowing clear narratives in STRs and robust responses to regulatory queries.[28]

Impact Analysis for NBFCs

Digital identity verification has moved from a peripheral convenience to a core compliance control for non-banking financial companies under the framework of the Prevention of Money-laundering Act, 2002. The discipline around customer due diligence is now inseparable from technologies such as video-based customer identification, Aadhaar offline verification, and reliance on structured registries like CKYCR. These tools influence not only how onboarding happens but also how records are created, retained, and reviewed in audits mandated by supervisory authorities. The legal standard remains tethered to obligations under "Section 12 of the Prevention of Money-laundering Act, 2002" and "Rule 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005", which require identification, verification, record-keeping, and ongoing monitoring. RBI's consolidated "Master Direction - Know Your Customer (KYC)" operationalizes this mandate and treats V-CIP as equivalent to face-to-face identification subject to defined

[24] Shekhar Vyas, "KYC Highlights and Challenges in India's AML Regime", 7 *International Journal of Law, Management & Humanities* 61 (2020).
[25] Yashaswini Sinha, "Tracing Beneficial Ownership: Corporate Veils and AML Duties", 15 *Journal of the Indian Law Institute* 97 (2021).
[26] FAQs on Master Direction on KYC, *available at:* https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=3782 (last visited on October 25, 2025).
[27] Pratik Prakash Dixit, "Conceptualising Interaction Between Cryptography and Law", 11 *NUJS Law Review* 119 (2018).
[28] Master Circular – Prevention of Money Laundering Act, 2002 – Obligations of NBFCs in Terms of Rules Notified Thereunder, *available at:* https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=530 (last visited on November 3, 2025).

safeguards. When embedded properly, digital identity lowers friction, extends reach, and sharpens risk controls, while also raising new questions about explainability and traceability of remote checks in an examiner setting.[29]

Efficiency and Inclusion Gains

Digital identity lowers entry barriers for customers and reduces onboarding time for NBFCs by allowing legitimate non-face-to-face relationships to commence with auditable comfort. RBI's KYC framework explicitly recognizes V-CIP and clarifies that it is on par with face-to-face, while Aadhaar-based approaches can be applied through OTP e-KYC for banks and offline verification for other regulated entities, supplemented by CKYCR pulls and DigiLocker e-documents. The Master Direction requires high-quality captures of proofs, tamper-evident audit trails, and centralized oversight, which together reduce repeat touchpoints during onboarding and periodic KYC. This matters especially for rural and semi-urban customers where travel costs, documentation scarcity, or branch access have historically impeded formal finance. RBI's treatment of accounts opened in non-face-to-face mode as high risk until V-CIP or physical verification is completed balances inclusion with prudence, and the June 2025 clarification on simple re-KYC via digital channels further smooths recurring interactions once initial identity assurance is established within a risk-based regime.

Risk Controls and Fraud Vectors

Remote identity brings its own adversaries in the form of deepfakes, replayed selfies, silicone-mask spoofing, and stitched synthetic profiles that evade naïve face-matching. The RBI rulebook anticipates this and forces calibrated countermeasures. V-CIP must be a live, informed, consent-based audio-visual interaction conducted by authorized officials. The process must enforce liveness detection, capture the customer's photograph, require the display and capture of the PAN image, and record geo-coordinates to tie the interaction to a physical location. Devices, networks, and applications used for V-CIP are subject to secure controls and time-stamped logs to create a verifiable trail for audits and dispute resolution. Offline Aadhaar verification is narrowed to an XML or QR artifact with a three-day validity window, curbing reuse across sessions. These controls reduce attack surface while preserving accessibility, and they set clear examiner expectations about reproducibility of checks, segregation of duties, and post-event retrievability of evidence that will be tested during thematic inspections and enforcement actions.[30]

Data Protection and Consent Management

The Digital Personal Data Protection Act, 2023 introduces a binding consent-first architecture that intersects directly with AML operations. Processing of KYC data must rest on a lawful ground under "Section 4 of the Digital Personal Data Protection Act, 2023", with valid consent defined in "Section 6", and purpose limitation, accuracy, and security obligations codified in "Section 8." An NBFC as data fiduciary remains accountable for processing done by KYC processors or identity vendors under "Section 8(2)", and must notify the Data Protection Board and affected principals of personal data breaches in the form and manner prescribed under "Section 8(6)." Contracting with verification vendors needs express allocation of duties, restrictions on sub-processing, security benchmarks, and deletion-triggered obligations so that operational practices map to statutory duties. The Act's approach to withdrawal of consent and erasure, tempered by retention permitted for legal compliance, ties back to AML record-keeping horizons and ensures that KYC archives are retained only for the period the law requires while remaining safeguarded against unauthorized disclosure.[31]

FATF Alignment and Supervisory Expectations

The Financial Action Task Force's "Guidance on Digital Identity" connects assurance levels of digital ID systems to Recommendation 10's customer due diligence requirements, encouraging supervisors to accept remote onboarding where system design, governance, and transaction monitoring combine to produce equivalent or stronger comfort than in-person workflows. Supervisory focus increasingly turns to how institutions calibrate liveness and spoof-resistance, whether model choices are documented and periodically validated, and whether logs can reconstruct decisions at scale. In India's 2024 mutual evaluation, the FATF community reviewed the effectiveness of preventive measures, which keeps pressure on regulators and entities to show that digital KYC does not create blind spots. Examiners look for demonstrable governance, including policies for risk-based supervision, exception handling, and traceable approvals. NBFC programs that align their V-CIP and e-KYC controls with FATF's assurance thinking, and that maintain high-fidelity audit logs, face fewer challenges when demonstrating equivalence and proportionality during on-site inspections and off-site reviews.[32]

Case Law and Jurisprudence

Judicial doctrine frames the permissible contours of identity processing and AML coercive powers, and these holdings influence how NBFCs design onboarding, record-keeping, and escalation. Privacy as a fundamental right directs proportionality analysis over KYC data flows, while the contours of PMLA enforcement define the gravity of breaches and the need for demonstrable compliance. The trajectory from recognition of informational privacy to validation of Aadhaar within limits, and onward to the endurance of PMLA's stringent bail and attachment standards, reflects a settlement that expects financial entities to be privacy-aware yet uncompromising on laundering risks. The more recent clarity on arrest powers after cognizance further aligns

[29] M. C. Mehanathan, *Law on Prevention of Money Laundering in India* 174 (LexisNexis, New Delhi, 1st edn., 2022).
[30] R. K. Naroola, Udayan Mukerji, et.al., *The Law of Prevention of Money Laundering* 163 (OakBridge, New Delhi, 1st edn., 2022).
[31] The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on November 2, 2025).
[32] Guidance on Digital Identity, *available at:* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (last visited on November 1, 2025).

investigative sequences with trial court control, a point relevant to how institutions handle summons, custody-related requests, and cooperation in proceedings.[33]

Justice K. S. Puttaswamy v. Union of India

In the case of "*Justice K. S. Puttaswamy v. Union of India*[34], a nine-judge bench unanimously affirmed that privacy is a fundamental right under Articles 14, 19, and 21. The petition questioned whether the Constitution guaranteed a justiciable right to privacy and whether prior decisions that denied such a right were good law. The Court overruled prior strands in "M.P. Sharma" and "Kharak Singh" to the extent inconsistent with this conclusion and set out an analytical structure for reviewing intrusions into privacy. The controlling frame emphasized that any infringement must satisfy legality, legitimate aim, proportionality, and procedural safeguards. The bench discussed informational privacy and acknowledged that evolving technology creates a need for a structured data protection regime covering collection, storage, and use. This recognition directly touches KYC data because identity attributes, biometric proxies, and transactional histories can reveal highly personal patterns. Under this doctrine, measures like digital onboarding, CKYCR queries, and Aadhaar offline verification must be anchored in legislative authority, be narrowly tailored to AML aims, and be implemented with safeguards like purpose limitation, limited retention, and auditability. Post-Puttaswamy, legislative and regulatory instruments such as the KYC Master Direction and later the DPDP Act help supply the legality and structure needed for proportional processing, while supervisory reviews look for practice-level evidence of necessity and safeguards rather than boilerplate policy statements, a shift visible in how regulators examine V-CIP recordings, consent artifacts, and data lineage in AML systems.[35]

Justice K. S. Puttaswamy (Aadhaar-5j) v. Union of India

In the case of "*K. S. Puttaswamy (Aadhaar-5J) v. Union of India*[36], the Supreme Court upheld the Aadhaar Act while striking particular provisions, carefully balancing state interests in targeted delivery and fraud prevention with privacy concerns. The majority sustained the system's constitutional validity but rejected the broad allowance for private sector mandatory authentication that had earlier enabled sweeping e-KYC uses. The judgment constrained private reliance on Aadhaar without explicit statutory backing and appropriate safeguards. Parliament then enacted the "Aadhaar and Other Laws (Amendment) Act, 2019", which permits voluntary use by individuals and controlled authentication by entities that meet security and privacy thresholds, with UIDAI empowered to specify modes including offline verification. This reset allowed banks and regulated firms to use Aadhaar with consent and alternatives, and RBI subsequently aligned its KYC Direction to reflect these options, limiting full Aadhaar e-KYC authentication to banks while permitting offline verification for other reporting entities. For NBFCs, the decision and the amendment together mean that Aadhaar can support digital onboarding when used voluntarily with informed consent, with offline artifacts or UIDAI-permitted authentication routed through a tightly governed regime. The framework rejects compulsion and emphasizes that identity proofing should coexist with choice and auditability in a way that satisfies proportionality and the AML objective of reliable identification.[37]

Vijay Madanlal Choudhary v. Union of India

In the case of "*Vijay Madanlal Choudhary v. Union of India*[38], the Supreme Court upheld the constitutional validity of the PMLA's core machinery including attachment under "Section 5", search and seizure under "Section 17", arrest under "Section 19", and the twin conditions for bail under "Section 45", while clarifying that ECIR is not equivalent to an FIR. The Court viewed these powers as having a reasonable nexus with the statute's objective of combating laundering of proceeds of crime. The decision signaled that AML processes stand on their own logic and that higher thresholds in bail and record seizure are legitimate. For NBFCs, this confirms that supervisory and investigative expectations will remain exacting, and that CDD failures can translate into serious exposure once a laundering trail is alleged. The Court's reading of "Section 24" on presumptions and its treatment of search, seizure, and arrest safeguards indicate that record integrity and evidentiary trails created during onboarding and monitoring will be scrutinized, including whether customer identities were verified through recognized methods and whether beneficial ownership and non-face-to-face risks were handled. Institutions that cannot show reliable digital identity checks, adequate logs, and documented escalations face compounded risk because the threshold to resist coercive measures remains high. The judgment has also influenced later benches discussing bail and custodial issues, reinforcing that compliance is simultaneously a defensive and a proactive imperative across the AML lifecycle.[39]

Tarsem Lal v. Directorate of Enforcement

In the case of "*Tarsem Lal v. Directorate of Enforcement*[40], the Supreme Court clarified the Enforcement Directorate's arrest power after a Special Court has taken cognizance of a PMLA complaint. The bench held that once cognizance is taken, the ED cannot proceed to arrest under "Section 19 of the PMLA" in that case and must seek custody from the court, with the trial procedure guided by the Code unless a PMLA provision expressly operates to the contrary. The Court explained the practical sequence around summons, warrants, and bonds, underlining that bond acceptance for appearance is not

---

[33] Justice K S Puttaswamy (Retd.) v. Union of India (Right to Privacy Judgment), *available at:* https://www.scobserver.in/wp-content/uploads/2021/10/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf (last visited on October 31, 2025).
[34] (2017) 10 SCC 1.
[35] Justice K S Puttaswamy (Retd.) and Another v. Union of India and Others, *available at:* https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf (last visited on October 30, 2025).
[36] (2019) 1 SCC 1.
[37] Justice K S Puttaswamy (Retd.) v. Union of India (Aadhaar Judgment, 2018), *available at:* https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf (last visited on October 29, 2025).
[38] 2022 SCC OnLine SC 929.
[39] Vijay Madanlal Choudhary v. Union of India, *available at:* https://indiankanoon.org/doc/14485072/ (last visited on October 28, 2025).
[40] 2024 INSC 434.

a grant of bail that triggers "Section 45" conditions. The holding refines the interface between investigation and trial, and it affects how institutions coordinate responses to process steps, including timely production of KYC records and digital artifacts when summoned. For NBFC compliance posture, the message is that while enforcement retains wide powers, the locus of custodial decisions after cognizance shifts to the Special Court, making procedural regularity and prompt cooperation central. The decision also aligns with a transparency-minded approach to enforcement, where arrest rationales, written reasons, and courtroom oversight reduce uncertainty for regulated entities involved as witnesses or custodians of records.[41]

Enforcement Trends and Regulatory Updates

Recent supervisory actions show that authorities measure digital KYC programs by outcomes rather than paper readiness. FIU-IND orders now narrate granular failings around client due diligence, beneficial owner determination, and suspicious transaction reporting, while RBI penalties cite non-adherence to KYC norms including periodic updation and risk categorization. This trend converts the conversation about V-CIP and offline Aadhaar from capability to evidentiary quality. Institutions that maintain strong, queryable logs, geo-tagged V-CIP recordings, and CKYCR-reconciled profiles handle inspections with fewer disputes. Amendments to the PML Rules in 2023 lowered beneficial ownership thresholds and tightened reliance on third-party due diligence, increasing the precision expected of digital identity workflows. The regulatory posture demands that technology choices be explainable, that consent records under the DPDP Act be auditable, and that vendor contracts faithfully mirror statutory duties imposed on data fiduciaries running KYC at scale.[42]

FIU-IND and RBI Actions on KYC Lapses

The Financial Intelligence Unit's March 1, 2024 order against Paytm Payments Bank reflects a willingness to characterize and penalize breaches that weaken AML reporting quality. The order demonstrates the level of specificity FIU-IND expects in systems that identify beneficial owners, screen customers, and furnish timely suspicious transaction reports, with explicit reference to obligations of reporting entities. RBI's press notices during October 2023 imposed monetary penalties on entities for non-compliance with KYC norms, including deficiencies in periodic updation and handling of non-face-to-face risks. These actions underline an expectation that regulated firms treat beneficial owner identification and monitoring as living controls rather than a one-time onboarding act, and that reliance on third parties or agents carries full responsibility back to the principal NBFC. For digital identity, this means that audit trails, exception workflows, and governance committee notes are as important as face-match accuracy, since enforcement now reads the story the logs can tell.[43]

Evolving RBI KYC Amendments

RBI's iterative amendments have clarified the use of non-face-to-face onboarding, V-CIP guardrails, and simplified re-KYC. The 2019 post-Aadhaar amendments allowed voluntary use with bank-led authentication and pushed other entities toward offline verification. Subsequent guidance standardized V-CIP with strict requirements around liveness, geo-tagging, and audit retention. The June 12, 2025 circular eased re-KYC by allowing digital completion through V-CIP or equivalent sources, provided the institution remains satisfied with risk classification and monitoring. For NBFCs, these steps create a consistent path to scale remote onboarding while staying inside PMLA and PML Rules. Success depends on combining these allowances with the 2023 amendments that tightened beneficial ownership tracing and with DPDP Act duties around lawful purpose, consent, and breach notification.[44]

Authority[45]	**Entity**	**Date**	**Issue**	**Takeaway**
FIU-IND	Paytm Payments Bank	March 1, 2024	Breaches of reporting entity obligations under PMLA including KYC-related failings and STR quality	FIU-IND expects verifiable BO identification, timely STRs, and end-to-end governance over onboarding and monitoring.
RBI	Pij People's Co-operative Bank Ltd	October 30, 2023	Non-compliance with KYC norms including periodic updation and risk processes	RBI enforces KYC discipline through monetary penalties where controls around customer profiling and updation slip.

Table 2: Recent enforcement actions related to KYC and AML.

[41] Enforcement Directorate's Power to Arrest Under PMLA After Special Court's Cognisance, *available at:* https://www.scobserver.in/cases/enforcement-directorates-power-to-arrest-under-pmla-after-special-courts-cognisance-tarsem-lal-v-directorate-of-enforcement/ (last visited on October 27, 2025).

[42] Dilip K. Sheth, *Treatise on Prevention of Money-Laundering Act, 2002: Law and Practice* 207 (Snow White Publications, Mumbai, 1st edn., 2024).

[43] Master Circular – Know Your Customer (KYC) Guidelines – Anti Money Laundering Standards – Prevention of Money Laundering Act, 2002 – Obligations of NBFCs in Terms of Rules Notified Thereunder, *available at:* https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1441 (last visited on October 26, 2025).

[44] Amendment to Master Direction on KYC, *available at:* https://www.rbi.org.in/Commonperson/english/scripts/Notification.aspx?Id=2968 (last visited on October 25, 2025).

[45] Akhilesh S. Dubey, *Treatise on PMLA: Law & Practice (In 2 Volumes)* 176 (Eastern Book Company, Lucknow, 1st edn., 2025).

Conclusion

The analysis demonstrates that digital identity has shifted from optional convenience to a mandatory competency in NBFC AML compliance. The 2023 revisions to the PML Rules tightened the definition and thresholds of beneficial ownership to more than 10 percent in companies and partnerships, increasing the depth of ownership tracing that NBFCs must perform during onboarding and throughout the relationship. RBI's Master Direction on KYC, reinforced by successive updates and FAQs, positions V-CIP as a true alternative to face-to-face verification, but only when specific controls—liveness detection, geo-tagging to confirm presence in India, officer-led capture of images, and direct source verification of identifiers—are implemented; printed copies of e-documents are explicitly disallowed during V-CIP to limit tampering. UIDAI's 2021 Regulations provide dual rails: online authentication for notified entities and paperless offline e-KYC (secure QR/XML) for broader use, enabling consent-based, cryptographically verifiable identity proofing without live calls to UIDAI. CKYCR's KYC Identifier regime reduces duplication by permitting consented, near-real-time retrieval of existing records, while FIU-IND timelines for CTRs and STRs push institutions to ensure that onboarding artefacts and monitoring signals are tightly coupled so suspicions can be articulated—and documented—promptly. FATF's Digital ID Guidance supplies the global benchmark by which Indian remote onboarding can be justified as standard- or even low-risk when assurance levels, performance, and spoof resistance are demonstrably high. In parallel, the DPDP Act clarifies that while erasure is a default right, AML statutes furnish a lawful basis to retain KYC records—often for ten years post-closure—so long as processing is purpose-limited, secured, and auditable.[46]

At the same time, digital identity introduces new risks that regulators increasingly scrutinize through an outcomes-based lens. Deepfakes, replay attacks, and synthetic identities exploit weaknesses in naïve face-matching or stale document reuse; RBI's insistence on concurrency checks, freshness windows for offline Aadhaar XML/QR, and end-to-end audit trails reflects this threat model. Effective NBFC programs therefore combine layered identity proofing (e.g., CKYCR pull + V-CIP + Aadhaar offline verification) with strong consent capture, masking of Aadhaar numbers, and vendor governance that contractually mirrors DPDP security and breach-notification duties. Data governance must bind together capture, storage, and retrieval of V-CIP recordings, CKYCR logs, QR/XML validation evidence, and e-document hashes within retention schedules that reconcile PMLA's ten-year horizon and DPDP's erasure triggers. Supervisory expectations now extend beyond checklists to reproducibility of decisions: institutions should be able to reconstruct why an identity was accepted, how beneficial ownership was determined under the >10 percent tests, and how a monitoring alert escalated into an STR within seven working days. When these ingredients are in place, digital identity materially reduces false onboarding, improves detection, accelerates reporting, and expands inclusion—especially in remote or underserved regions—without compromising legal defensibility. The strategic implication is clear: digital identity is not a point solution but a compliance architecture, and competitive NBFCs will treat it as a governed, continuously validated capability aligned to FATF assurance levels, RBI operational guardrails, UIDAI trust services, CKYCR data quality, and DPDP accountability.

Suggestions

Building on this examination of how digital identity verification reshapes NBFC compliance obligations, the following targeted actions translate doctrine into day-to-day practice:[47]

- Institutionalize a "triple-rail" onboarding playbook. For retail onboarding, default to CKYCR download (with consent), plus Aadhaar paperless offline e-KYC (secure QR/XML), plus V-CIP for liveness and geo-presence. Define when one or two rails suffice (e.g., low-risk, recent CKYCR record) and when all three are mandatory (e.g., higher-risk geographies or products). Encode these combinations as policy rules in onboarding systems so deviations generate approvals and audit notes.
- Make beneficial ownership discovery "10-percent-first." Re-design forms and system fields to capture ownership/control at 1% granularity with prompts when any natural person crosses >10% (companies/partnerships). Integrate document capture for board resolutions, partnership deeds, and control rights and tie them to V-CIP review where feasible. Use exception queues for complex structures (multi-layer entities, trusts) and require second-line concurrence before account activation.
- Embed consent artifacts everywhere identity data moves. Capture granular, revocable consent for CKYCR pulls, Aadhaar offline verification, and e-document retrieval, with timestamps, purpose tags, and officer IDs. Store hash-linked consent receipts alongside KYC artifacts so that every regulatory query can be answered with a single evidentiary bundle. Auto-block reuse of identity data for unrelated purposes unless a new consent pathway is completed.
- Harden V-CIP against spoofing by design. Enforce device integrity checks, active liveness challenges (blink/turn/phrase), and GPS/IP concordance with "in-India" checks. Prohibit screen-sharing and restrict copy-paste into capture fields; always verify PAN/e-PAN directly with the issuer API during the call. Add a concurrent quality-control layer that rejects sessions with artefacts (frame drops, glare, mismatched lip-sync) before account opening.
- Operationalize the ten-year retention rule with DPDP alignment. Maintain a single retention schedule that tags each artifact (V-CIP files, QR/XML packages, CKYCR logs) with its legal basis and end-of-life date. Automate legal holds for ongoing investigations while preventing over-retention elsewhere; produce deletion certificates on expiry. Ensure breach-response runbooks notify the Board and affected customers

[46] FinMin Tightens PMLA Rules, Brings Partners With 10% Stake Under Its Purview, *available at:* https://m.economictimes.com/news/economy/policy/finmin-tightens-pmla-rules-brings-partners-with-10-stake-under-its-purview/articleshow/103436322.cms (last visited on November 3, 2025).

[47] R. K. Naroola, *Compliance Handbook on PMLA for Financial Institutions* 188 (OakBridge, New Delhi, 1st edn., 2022).

and preserve volatile evidence without breaking erasure obligations.

- Create a CKYCR "data quality and recency" gate. Accept downloads only if the profile is complete, current, and meets present-day OVD/e-document norms; otherwise trigger targeted refresh. Record structured reasons whenever re-collection is performed to satisfy Rule 9 and RBI FAQs. Feed CKYCR update notifications into the customer 360 so address/BO changes auto-spawn re-KYC via V-CIP.
- Stand up a model-risk program for identity analytics. Maintain documented performance metrics for face-match, liveness, and fraud scoring models, including periodic bias and error-rate reviews. Calibrate thresholds by segment (product, geography, age) and log every override with rationale. Validate vendor claims via A/B tests and independent red-team exercises that simulate deepfakes and replay attacks.
- Link onboarding to FIU-IND reporting pipelines. Design STR drafting templates that pull identity artefacts (V-CIP timestamps, QR/XML verification logs, consent records) into a narrative automatically. Enforce timers that remind investigators of the seven-working-day STR window once suspicion is formed. For CTRs, reconcile onboarding dates and cash profiles monthly and escalate anomalies to the Principal Officer.
- Strengthen vendor and API governance. For KYC providers (video, OCR, QR/XML validation), stipulate DPDP-grade security, sub-processor transparency, breach notification SLAs, and deletion timelines. Require per-session audit logs and cryptographic signatures on outputs; reject "black-box" models without exportable evidence. Conduct annual audits that include code-walkthroughs of SDKs and penetration tests of V-CIP capture apps.
- Train, test, and evidence. Run quarterly exercises where teams must reconstruct an onboarding case end-to-end for an internal "mock inspection", including BO discovery at the >10% threshold, CKYCR consent, V-CIP artifacts, and STR rationale. Track error themes to update SOPs and retrain staff. Publish governance minutes that show how regulatory updates (RBI KYC amendments, UIDAI advisories) are translated into controls within defined implementation timelines.

Bibliography

Books:

- Akhilesh S. Dubey, Treatise on PMLA: Law & Practice (In 2 Volumes) (Eastern Book Company, Lucknow, 1st edn., 2025).
- Commercial Law Publishers Editorial Team, Commentary on the Prevention of Money Laundering Act, 2002 (Commercial Law Publishers, New Delhi, 1st edn., 2024).
- Dilip K. Sheth, Treatise on Prevention of Money-Laundering Act, 2002: Law and Practice (Snow White Publications, Mumbai, 1st edn., 2024).
- Dr. Shamsuddin, Commentary on the Prevention of Money Laundering Act, 2002 (Commercial Law Publishers, New Delhi, 1st edn., 2024).
- Indian Institute of Banking & Finance, Non-Banking Financial Companies (Taxmann Publications, New Delhi, 1st edn., 2025).
- Indian Institute of Corporate Affairs Faculty, Data Protection and Financial Services in India (OakBridge, New Delhi, 1st edn., 2021).
- M. C. Mehanathan, Law on Prevention of Money Laundering in India (LexisNexis, New Delhi, 1st edn., 2022).
- R. K. Naroola, Compliance Handbook on PMLA for Financial Institutions (OakBridge, New Delhi, 1st edn., 2022).
- R. K. Naroola, Udayan Mukerji, et al., The Law of Prevention of Money Laundering (OakBridge, New Delhi, 1st edn., 2022).
- Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins, New Delhi, 1st edn., 2018).
- Rajat Bhatia, Video KYC, V-CIP and Digital Onboarding: Legal Standards and Controls (Bloomsbury Professional India, New Delhi, 1st edn., 2021).
- Reserve Bank Compliance Forum, KYC, CKYCR & Digital Identity for REs (Taxmann Publications, New Delhi, 1st edn., 2022).
- Shankkar Aiyar, Aadhaar: A Biometric History of India's 12-Digit Revolution (Westland, Chennai, 1st edn., 2017).
- Somesh Arora, Prevention of Money Laundering Act, 2002: A Commentary (OakBridge, New Delhi, 1st edn., 2023).
- Taxmann Editorial Board, Money Laundering Law Manual (Taxmann Publications, New Delhi, 1st edn., 2023).

Statutes:

- The Aadhaar (Authentication and Offline Verification) Regulations, 2021 (No. G.S.R. 99(E) of 2021)
- The Aadhaar and Other Laws (Amendment) Act, 2019 (Act No. 14 of 2019)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Prevention of Money-laundering (Maintenance of Records) Rules, 2005 (G.S.R. 693(E) of 2005)

- The Prevention of Money-laundering Act, 2002 (Act No. 15 of 2003)

Articles:

- Nupur Chowdhury, "Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy", 11 NUJS Law Review 96 (2018).
- Pratik Prakash Dixit, "Conceptualising Interaction Between Cryptography and Law", 11 NUJS Law Review 119 (2018).
- Renuka Thapar, "e-KYC and Financial Inclusion: Regulatory Design for Trust and Risk", 9 NLSIU National Law School Journal 88 (2019).
- Shekhar Vyas, "KYC Highlights and Challenges in India's AML Regime", 7 International Journal of Law, Management & Humanities 61 (2020).
- Vidushi Marda, Amber Sinha, "FinTech Lending in India: Taking Stock of Implications for Privacy and Autonomy", 18 Indian Journal of Law and Technology 72 (2022).
- Vrinda Bhandari, Renuka Sane, "A Critique of Aadhaar Framework", 31 National Law School of India Review 58 (2019).
- Yashaswini Sinha, "Tracing Beneficial Ownership: Corporate Veils and AML Duties", 15 Journal of the Indian Law Institute 97 (2021).

Websites:

- Amendment to Master Direction on KYC, available at: https://img1.digitallocker.gov.in/circulars/RBI_master_circular_on_eKYC_09.01.2020.PDF (last visited on November 1, 2025).
- Amendment to Master Direction on KYC, available at: https://www.rbi.org.in/Commonperson/english/scripts/Notification.aspx?Id=2968 (last visited on October 25, 2025).
- Enforcement Directorate's Power to Arrest Under PMLA After Special Court's Cognisance, available at: https://www.scobserver.in/cases/enforcement-directorates-power-to-arrest-under-pmla-after-special-courts-cognisance-tarsem-lal-v-directorate-of-enforcement/ (last visited on October 27, 2025).
- FAQs on Master Direction on KYC, available at: https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=3782 (last visited on October 25, 2025).
- FinMin Tightens PMLA Rules, Brings Partners With 10% Stake Under Its Purview, available at: https://m.economictimes.com/news/economy/policy/finmin-tightens-pmla-rules-brings-partners-with-10-stake-under-its-purview/articleshow/103436322.cms (last visited on November 3, 2025).
- Guidance on Digital Identity, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf (last visited on October 28, 2025).
- Justice K S Puttaswamy (Retd.) and Another v. Union of India and Others, available at: https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf (last visited on October 30, 2025).
- Justice K S Puttaswamy (Retd.) v. Union of India (Aadhaar Judgment, 2018), available at: https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf (last visited on October 29, 2025).
- Justice K S Puttaswamy (Retd.) v. Union of India (Right to Privacy Judgment), available at: https://www.scobserver.in/wp-content/uploads/2021/10/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf (last visited on October 31, 2025).
- Kharak Singh v. State of Uttar Pradesh, available at: https://indiankanoon.org/doc/290623/ (last visited on October 30, 2025).
- Master Circular - Know Your Customer (KYC) Guidelines - Anti Money Laundering Standards - Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in Terms of Rules Notified Thereunder, available at: https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1441 (last visited on October 26, 2025).
- Master Circular - Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in Terms of Rules Notified Thereunder, available at: https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=530 (last visited on November 3, 2025).
- Master Direction - Know Your Customer (KYC) Direction, 2016, available at: https://www.rbi.org.in/commonman/English/scripts/notification.aspx?id=2607 (last visited on November 3, 2025).
- PML (Maintenance of Records) Rules, 2005, available at: https://fiuindia.gov.in/files/AML_Legislation/notification.html (last visited on October 26, 2025).
- The Aadhaar (Authentication and Offline Verification) Regulations, 2021, available at: https://uidai.gov.in/images/The_Aadhaar_Authentication_and_Offline_Verifications_Regulations_2021.pdf (last visited on October 27, 2025).
- The Aadhaar and Other Laws (Amendment) Act, 2019, available at: https://uidai.gov.in/images/news/Amendment_Act_2019.pdf (last visited

on October 29, 2025).

- The Digital Personal Data Protection Act, 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on November 2, 2025).
- The Prevention of Money-Laundering Act, 2002, available at: https://enforcementdirectorate.gov.in/sites/default/files/Act%26rules/THE%20PREVENTION%20OF%20MONEY%20LAUNDERING%20ACT%2C%202002.pdf (last visited on November 2, 2025).
- Vijay Madanlal Choudhary v. Union of India, available at: https://indiankanoon.org/doc/14485072/ (last visited on October 28, 2025).