KNOW YOUR CUSTOMER (KYC), ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT)

(Pursuant to the Prevention of Money-Laundering Act, 2002, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005

Regulatory Basis	RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time)
Approving Authority	Board of Directors
Review Frequency	At least annually and earlier where required

1. Introduction & Regulatory Framework

Comero Leasing and Financials Private Limited (hereinafter referred to as "the Company" or "RE") is committed to maintaining the highest standards of integrity, transparency, and regulatory alignment. As a Non-Banking Financial Company (NBFC), the Company establishes this Policy in strict compliance with:

- **The Prevention of Money-Laundering Act, 2002 (PMLA)** and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time.
- **The RBI Master Direction – Know Your Customer (KYC) Direction, 2016** (RBI/DBR/2015-16/18 Master Direction DBR.AML.BC. No.81/14.01.001/2015-16), as updated from time to time.
- **The Unlawful Activities (Prevention) Act, 1967 (UAPA)** and The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act).
- **Operational guidelines and reporting directives** issued by the Financial Intelligence Unit – India (FIU-IND).

Purpose

- To prevent the Company's credit, leasing, and financial products/services from being utilized, directly or indirectly, for money laundering, predicate offenses, or terrorist financing activities.
- To lay down structured Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), transaction monitoring, and statutory reporting frameworks.
- To embed a robust Risk-Based Approach (RBA) into all operational and client onboarding workflows in alignment with RBI mandates.

2. Objective & Scope

- **Objective:** To establish an end-to-end, proportionate, and risk-based framework for customer identification, verification, beneficial ownership determination, risk categorization, transaction monitoring, record preservation, regulatory reporting, and internal controls.
- **Scope:** This Policy applies universally across the Company to all prospective, existing, and former customers/borrowers/lessees; Beneficial Owners (BOs), authorized signatories, powers-of-attorney holders, co-borrowers, and guarantors; Lending Service Providers (LSPs), Digital Lending Platforms (DLPs), Business Correspondents (BCs), and Direct Selling Agents (DSAs) engaged by the Company; and all products, services, delivery channels, and digital onboarding platforms operated by or on behalf of the Company.

3. Key Definitions

- **Customer Due Diligence (CDD):** The process of identifying and verifying the customer's identity and address using reliable, independent source documents, data, or information, as well as identifying and verifying beneficial owners.
- **Central KYC Records Registry (CKYCR):** A centralized repository established to receive, store, safeguard, and retrieve digital KYC records of customers across the financial sector.
- **Officially Valid Document (OVD):** Passport, Driving License, Proof of possession of Aadhaar number (in masked form), Voter's Identity Card issued by the Election Commission of India, Job card issued by NREGA duly signed by an officer of the State Government, and Letter issued by the National Population Register containing details of name and address.
- **Digital KYC:** Capturing a live photo of the customer and an OVD/officially valid proof, along with latitude/longitude and timestamp, by an authorized officer of the RE as per prescribed procedures.
- **Equivalent e-Document:** An electronic copy of an OVD issued by the issuing authority including documents issued to DigiLocker, bearing digital signatures or e-signatures.
- **Politically Exposed Persons (PEPs):** Individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., Heads of State/Government, senior politicians, senior judicial/military officials, senior executives of state-owned corporations). Requirements extend to family members and close associates.
- **Video-based Customer Identification Process (V-CIP):** An interactive audio-visual digital process for remote onboarding and CDD complying with strict RBI security and encryption protocols.

4. Governance Structure & Designated Officers

The Board of Directors holds ultimate oversight for the AML/CFT compliance framework and has appointed dedicated senior officials to ensure operational independence and compliance enforcement:

A. Principal Officer — Mr. Rahul Kumar Jha (Chief Financial Officer)

- Monitoring transactions, reviewing automated alerts, and evaluating internal suspicious activity reports.
- Determining transaction suspicion and ensuring timely filing of Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), and other regulatory filings with FIU-IND.
- Serving as the primary liaison officer with FIU-IND, RBI, and law enforcement agencies while maintaining strict confidentiality regarding reporting activities.

B. Designated Director — Mr. Rishabh Kanojia (Director)

- Ensuring overall implementation of obligations imposed under Chapter IV of the PMLA and the PML Rules.
- Allocating adequate operational, technological, and human resources for the effective implementation of the KYC/AML/CFT framework.
- Presenting quarterly AML/CFT compliance and risk evaluation reports to the Board of Directors.

5. Customer Acceptance Policy (CAP)

The Company enforces strict acceptance parameters prior to establishing any business relationship:

- **No Anonymous Accounts:** No account shall be opened, and no credit or leasing facility executed, in an anonymous, fictitious, or benami name.
- **Mandatory Sanctions Screening:** Real-time pre-onboarding automated screening of all prospective customers, beneficial owners, and directors/partners must be performed against United Nations Security Council Sanctions Lists (UNSCL), MHA Designated Lists under UAPA, WMD Act lists, and RBI/FIU warning lists.
- **Inability to Complete CDD:** Where the Company is unable to apply appropriate CDD measures, verify identity, or obtain required information, it shall not open the account or commence business relations. If a relationship already exists, the Company shall consider filing an STR and terminating the relationship.
- **Non-Discrimination & Accessibility:** Aadhaar is entirely voluntary for general commercial KYC. Onboarding shall never be denied solely due to a customer's refusal to furnish Aadhaar, provided another valid OVD is submitted. Rejection of Persons with Disabilities

(PwDs) is strictly prohibited, and any rejection must be escalated to the Principal Officer with written reasons recorded.

6. Customer Identification Procedure (CIP) & Onboarding Modalities

A. Central KYC Records Registry (CKYCR)

- The Company shall query CKYCR using the customer's KYC Identifier or official search parameters. Upon customer consent, retrieved KYC documents shall be utilized without demanding duplicate physical copies unless information is outdated.
- **10-Day Mandatory Upload Rule:** In accordance with PML Rule 9(1A), the Company shall upload the customer's KYC profile and e-documents to CKYCR within 10 days of establishing the business relationship.

B. Permitted Onboarding Avenues

- Direct verification of physical OVDs or validated Equivalent e-Documents retrieved via DigiLocker.
- **Aadhaar OTP-based e-KYC:** Permitted subject to explicit consent. Non-face-to-face OTP e-KYC accounts are subject to an aggregate credit limit of ₹60,000 per financial year and mandatory completion of full CDD within 1 year.
- **Aadhaar Face Authentication:** Biometric matching in compliance with UIDAI specifications.
- **V-CIP Framework:** Remote video onboarding subject to live interaction, liveness checks (excluding mandatory specific facial gestures for PwDs), concurrent geo-tagging, direct fetching of PAN from NSDL/ITD, and secure end-to-end encrypted storage.

7. Risk Categorization Matrix & Periodic Updation

Customers shall be categorized into Low, Medium, and High Risk based on customer profile, business activity, geographical presence, legal structure, and product exposure.

Risk Category	Customer Profile / Target Profile Examples	Statutory Periodic Updation Cycle
Low Risk	Salaried employees, government bodies, statutory corporations, low-net-worth individuals with clear domestic income streams.	Once every 10 Years

Medium Risk	Independent contractors, high-volume domestic traders, cash-intensive sole proprietorships, entities with non-complex structures.	Once every 8 Years
High Risk	Politically Exposed Persons (PEPs), non-residents, complex trust/corporate legal structures, high-net-worth individuals, foreign source exposure.	Once every 2 Years

Transition Grace Period for Low-Risk Updation

For Low-Risk individual customers where periodic updation becomes due, account operations shall not be abruptly blocked. A transition grace period allows continued operations provided the updation is completed within 1 year of the due date or by June 30, 2026, whichever is later, during which regular transaction monitoring continues.

8. Beneficial Ownership (BO) & Enhanced Due Diligence (EDD)

A. Beneficial Ownership Identification Thresholds

- **Companies:** Natural people holding greater than 10% of shares, capital, or profits, or exercising control through voting rights or agreements.
- **Partnerships & Unincorporated Entities:** Natural persons holding greater than 10% of property, capital, or profits.
- **Trusts:** Identification of the Settlor/Author, Trustees, Beneficiaries with 10% or more interest, and any natural person exercising ultimate effective control.
- **Unincorporated Association / BOI:** Natural persons holding greater than 15% of property, capital, or profits.
- **Senior Managing Official:** Where no natural person is identified under ownership or control tests, the natural person holding the position of Senior Managing Official (SMO) shall be identified as the BO.

B. Enhanced Due Diligence (EDD)

- **PEP Approvals:** Senior Management / Director approval is mandatory prior to onboarding PEPs or transitioning an existing client to PEP status.
- **Source of Funds & Wealth:** Verification of legitimate sources of wealth and origin of funds for high-net-worth and high-risk accounts.

- **Specified Transactions (Section 12AA PMLA):** Examination of the background, financial standing, purpose, and underlying economic rationale of unusual transactions prior to execution.

9. Transaction Monitoring & Occasional Thresholds

- **Ongoing Scrutiny:** All customer transactions shall be continuously monitored against their declared risk profile, income standing, and historical volume.
- **Occasional Transactions Threshold:** Identity verification shall be enforced for occasional transactions of ₹50,000 or more (whether conducted as a single transaction or through several apparently connected transactions).
- **NBFC Red Flag Monitoring:** Special automated monitoring rules shall track early loan closures/prepayments using cash or unverified third-party accounts, multiple loan applications sharing identical phone numbers/addresses, and repayments originating from high-risk foreign jurisdictions.

10. Reporting Obligations to FIU-IND

All statutory reporting duties fall under the direct authority of the Principal Officer.

- **Suspicious Transaction Reports (STRs):** Submitted electronically via FINnet within 7 working days of the Principal Officer arriving at a conclusion that a transaction is suspicious in nature.
- **Cash Transaction Reports (CTRs):** Monthly filing of all cash transactions exceeding ₹10 Lakhs (or foreign equivalent) by the 15th day of the succeeding month.
- **Non-Profit Organisation Reports (NPORs):** Monthly filing of receipts by non-profit organizations exceeding ₹10 Lakhs by the 15th day of the succeeding month.
- **Cross-Border Wire Transfer Reports (CBWTRs):** Filed by the 15th day of the succeeding month for foreign wire transfers exceeding ₹5 Lakhs.
- **Prohibition of Tipping-Off:** Company employees and officers are strictly prohibited from disclosing to the customer or any third party that an STR or alert is under review or filed with FIU-IND.

11. Record Keeping & Data Preservation

- **Transaction Records:** Maintained for at least 5 years from the date of the transaction.
- **CDD & Account Files:** Customer identity, BO records, account files, and business correspondence shall be preserved for at least 5 years after the business relationship has ended or the account has been closed, whichever is later.

- **V-CIP Records:** Audio-video recordings and digital logs shall be retained for a minimum of 5 years.
- **Reconstruct ability:** Records must be stored in a structured format enabling step-by-step reconstruction of individual transactions for production to statutory authorities upon lawful requests.

12. Internal Controls, Independent Audit, and Training

- **Independent Internal Audit:** The internal audit team (or external specialized audit firm) shall conduct an annual assessment of the Company's KYC/AML/CFT compliance, sanctions screening software, CKYCR upload efficiency, and STR reporting integrity. Findings shall be submitted to the Audit Committee of the Board.
- **Employee Training:** Periodic, role-based training programs shall be conducted for all onboarding, credit, operational, and compliance staff covering AML red flags, digital onboarding rules, and tipping-off regulations.

13. Annual Policy Review & Risk Assessment

- **Annual Policy Review:** This policy shall be reviewed, updated, and approved by the Board of Directors at least once every calendar year or immediately upon major regulatory amendments by the RBI, PMLA Rules, or FIU-IND.
- **Enterprise ML/TF Risk Assessment:** The Company shall conduct a periodically documented ML/TF risk assessment covering its customer base, products, delivery channels, and geographic exposure to calibrate its risk-based AML controls effectively.