

LAKME INVESTMENT AND FINANCE LIMITED

Regd Office: No. 1, Anna Pillai Street, Chennai – 600 001.

Corporate Office: No.1, Padiyur Road, Pudupatti, Dindigul – 624 005.

CIN: U65993TN1995PLC033288 | Email ID: compliance@lakmefinance.com | Mobile No: 8925975497

ANTI MONEY LAUNDERING (AML) AND KNOW YOUR CUSTOMER (KYC) POLICY

Board Approved Date: 20-03-2026

SI No	INDEX	Page
1	PREAMBLE	2
2	OBJECTIVE	3
3	REGULATORY FRAMEWORK	3
4	APPLICABILITY	3
5	GOVERNANCE FRAMEWORK	3
6	CUSTOMER ACCEPTANCE POLICY (CAP)	4
7	CUSTOMER IDENTIFICATION PROGRAM (CIP)	4
8	VIDEO- BASED CUSTOMER IDENTIFICATION PROCESS (V-CIP)	6
9	CUSTOMER RISK CATEGORIZATION FRAMEWORK	6
10	AADHAAR LINKED MOBILE NUMBER CHANGE MANAGEMENT	9
11	MONITORING AND REPORTING OF TRANSACTIONS	9
12	ENHANCED DUE DELIGENCE (“EDD”)	9
13	ONGOING DUE DELIGENCE	10
14	RISK MANAGEMENT	10
15	CUSTOMER EDUCATION	10
16	EMPLOYEE TRAINING	10
17	APPOINTMENT OF PRINCIPAL OFFICER	11
18	MAINTENANCE OF RECORDS	11
19	INFORMATION TO BE PRESERVED	11
20	REPORTING TO FINANCIAL INTELLIGENT UNIT-INDIA (“FIU-IND”)	11
21	DATA CONFIDENTIALITY AND SECURITY	12
22	POLICY REVIEW	12
23	BOARD APPROVAL	12

1. PREAMBLE

Lakme Investment and Finance Limited ("the Company"), a Non-Banking Financial Company – Base Layer (NBFC-BL), is committed to maintaining the highest standards of integrity, transparency, and regulatory compliance in all its business operations. The Company recognizes that an effective Anti-Money Laundering (AML) and Know Your Customer (KYC) framework is fundamental to safeguarding the financial system against misuse for unlawful activities like money laundering, terrorist financing, proliferation financing, fraud, identity theft etc.

This Policy has been formulated in accordance with the provisions of the Prevention of Money Laundering Act, 2002 (PMLA), the rules framed thereunder, and the guidelines issued by the Reserve Bank of India (RBI), including the Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time, along with all other applicable laws, regulations, circulars, and notifications issued by competent regulatory authorities.

The objective of this Policy is to establish a robust risk-based framework for customer acceptance, customer identification, customer due diligence (CDD), beneficial ownership verification, ongoing monitoring of transactions, record maintenance, reporting of prescribed transactions to the Financial Intelligence Unit – India (FIU-IND), and implementation of appropriate internal controls. The Policy also seeks to ensure that the Company conducts business only with legitimate customers whose identities and sources of funds can be reasonably established, thereby protecting the Company from reputational, operational, legal, and compliance risks.

The Company adopts a risk-based approach to customer onboarding and monitoring by classifying customers into appropriate risk categories based on factors such as customer profile, nature of business, geographical location, products and services availed, transaction patterns, and other relevant risk indicators. Enhanced Due Diligence (EDD) shall be applied wherever warranted in accordance with applicable regulatory requirements.

This Policy shall be applicable to all Directors, Key Managerial Personnel, employees, branches, business correspondents (where applicable), outsourcing service providers, Digital Lending Service Providers (LSPs), agents, and any other persons acting on behalf of the Company. Every employee shall be responsible for ensuring strict compliance with this Policy and promptly reporting any suspicious transactions or activities in accordance with the prescribed internal reporting mechanisms. The Board of Directors shall periodically review this Policy to ensure its continued effectiveness and alignment with the evolving regulatory framework, emerging financial crime risks, and the business operations of the Company. Any amendments to this Policy shall be approved by the Board or by such authority as may be authorized by the Board, in accordance with applicable laws and RBI directions.

This Policy shall be read in conjunction with the Company's Customer Acceptance Policy (CAP), Customer Identification Procedures (CIP), Customer Due Diligence (CDD) framework, Risk Management Policy, Digital Lending Policy, Fair Practices Code, Information Security Policy, and other internal policies governing compliance and risk management.

2. OBJECTIVE

The objective of this Policy is to ensure that Lakme Investment and Finance Limited ("Company") is not used, intentionally or unintentionally, for:

- a. Money Laundering;
- b. Terrorist Financing;
- c. Fraudulent Activities;
- d. Identity Theft;
- e. Financial Crime;
- f. Sanctions Evasion;
- g. Other unlawful activities.

The Policy establishes a risk-based framework for customer acceptance, identification, monitoring, due diligence, reporting and regulatory compliance.

3. REGULATORY FRAMEWORK

This Policy is framed in accordance with:

- a. Prevention of Money Laundering Act, 2002;
- b. Prevention of Money Laundering Rules, 2005;
- c. RBI Master Direction – Know Your Customer (KYC) Direction, 2016, as amended;
- d. RBI Master Directions applicable to NBFCs;
- e. Financial Intelligence Unit – India (FIU-IND) guidelines;
- f. FATF Recommendations;
- g. Other applicable laws and regulations.

4. APPLICABILITY

This Policy shall apply to:

- a. All customers;
- b. Directors;
- c. Employees;
- d. Agents;
- e. Recovery personnel;
- f. Business sourcing partners;
- g. Lending Service Providers (LSPs);
- h. Outsourced service providers.

5. GOVERNANCE FRAMEWORK

5.1 Board of Directors

The Board shall:

- a. Approve AML/KYC Policy;
- b. Review AML compliance annually;
- c. Review high-risk AML matters;
- d. Ensure adequate AML resources.

5.2 Loan Committee

The Loan Committee shall periodically review:

- a. AML compliance;
- b. STR (Suspicious Transaction Report) reporting framework;
- c. Internal audit findings;
- d. Regulatory observations.

5.3 Principal Officer

The Company shall appoint a Principal Officer responsible for:

- AML monitoring;
- STR reporting;
- FIU coordination;
- Regulatory communication.

5.4 Designated Director

A Designated Director shall be appointed under PMLA (Prevention of Money Laundering Act) requirements.

6 . CUSTOMER ACCEPTANCE POLICY (CAP)

The Company shall ensure:

- a. No anonymous accounts;
- b. No fictitious names;
- c. No benami relationships;
- d. No onboarding without KYC;
- e. Identification of beneficial owners;
- f. Risk-based customer categorization.

The Company may reject onboarding where:

- a. KYC is incomplete;
- b. Information is misleading/false
- c. Customer appears on sanctions lists;
- d. AML concerns exist.

7 . CUSTOMER IDENTIFICATION PROGRAM (CIP)

Before establishing a relationship, the Company shall verify:

- a. Identity;
- b. Address;
- c. PAN;
- d. Beneficial ownership;
- e. Purpose of relationship;
- f. Source of funds where applicable.

Verification may be completed through:

- a. Physical KYC;
- b. Digital KYC;
- c. Aadhaar Offline Verification;
- d. V-CIP;
- e. CKYCR records.

7.1 KYC Documents – Individuals

Proof of Identity

Anyone of the following:

- a. PAN Card;
- b. Aadhaar Card;
- c. Passport;
- d. Voter ID;
- e. Driving License;
- f. Any Officially Valid Document (“OVD”) permitted under RBI guidelines.

Proof of Address

Any one of the following:

- a. Aadhaar Card;
- b. Passport;
- c. Utility bill not older than two months;
- d. Bank statement not older than 6 months;
- e. Registered rent agreement;
- f. Any other permitted by RBI.

Additional Documents

- a. Recent photograph;
- b. MSME Certificate where applicable;
- c. Income proof and bank statements as required.

7.2 KYC Documents – Non-Individuals

A. Companies/ LLPs

- a. Certificate of Incorporation;
- b. Memorandum & Articles of Association;
- c. PAN of the Company;
- d. Board Resolution authorizing opening of account and borrowing;
- e. List of Directors and shareholders;
- f. Beneficial ownership declaration;
- g. Address proof of registered office;
- h. KYC of authorized signatories.
- i. LEI for Loan amount of Rs.5 Cr or above
- j. Name of existing bankers /lenders with consent for seeking opinion reports from them

B. Partnership Firms

- a. Registration Certificate;
- b. PAN of Firm;
- c. Partnership Deed/ agreement;
- d. Address proof;
- e. Authorization letter;
- f. KYC of all partners and authorized signatories.

C. Trusts / Societies / NGOs

- a. Registration Certificate;
- b. PAN;
- c. Trust Deed / Bye-laws;
- d. List of trustees/office bearers;
- e. KYC of all trustees and authorized signatories;
- f. Beneficial ownership details.

8. VIDEO- BASED CUSTOMER IDENTIFICATION PROCESS (V-CIP)

Where permitted under RBI regulations, the Company may undertake V-CIP.

V-CIP shall include:

- a. Live video interaction;
- b. Geo-tagging;
- c. Liveness verification;
- d. OVD verification;
- e. Recording retention.

9. CUSTOMER RISK CATEGORIZATION FRAMEWORK

The Company shall adopt a Risk-Based Approach (“RBA”) for categorizing customers into High Risk, Medium Risk and Low Risk categories based on the nature of customer, business activity, geographic exposure, exposure for NBFC, transaction pattern, source of funds and other relevant risk indicators.

Customer risk categorization shall be carried out at the time of onboarding and reviewed periodically.

9.1 Parameters for Risk Assessment

The following factors should be considered while assessing customer risk:

A. Customer Profile Risk

- a. Nature of customer (individual, company, trust, partnership, NGO etc.)
- b. Occupation/business activity
- c. Politically Exposed Person (“PEP”) status
- d. Ownership structure and beneficial ownership complexity
- e. Financial background and source of income
- f. level of exposure/VaR

B. Geographic Risk

- a. Customer located in high-risk jurisdictions
- b. Countries identified by FATF for AML deficiencies
- c. Areas with higher incidence of fraud, terrorism financing or illegal activities

C. Product / Service Risk

- a. Type of loan product availed
- b. Non-face-to-face onboarding
- c. Cash-intensive business models
- d. Complex repayment structures

D. Transaction Risk

- a. Unusual transaction behavior
- b. Sudden increase in turnover or repayment pattern
- c. Frequent cash transactions
- d. Multiple linked accounts or layered transactions

E. Channel Risk

- a. Digital onboarding
- b. Third-party sourced applications
- c. Remote customer onboarding channels

9.2 Customer Risk Categories:**A. Low Risk Customers**

Customers whose identity and source of income can be easily verified and who pose minimal AML/CFT (Anti-Money Laundering and Combating the Financing of Terrorism) risk may be categorised as Low Risk.

Illustrative categories:

- a. Salaried employees with stable income;
- b. Individuals with small-ticket retail loans;
- c. Existing customers with satisfactory repayment track record;
- d. Government departments and government-owned entities;
- e. Customers receiving salary through banking channels.

Due Diligence Requirements:

- a. Standard Customer Due Diligence (“CDD”);
- b. Basic KYC verification;
- c. Periodic KYC updation every 10 years or as prescribed by RBI.

B. Medium Risk Customers

Customers with moderate risk exposure due to business nature, transaction volume or ownership structure may be categorised as Medium Risk.

Illustrative categories:

- a. Self-employed individuals;
- b. SMEs and proprietorship businesses;
- c. Partnership firms;
- d. Customers with moderate cash transactions;
- e. Non-individual entities with simple ownership structure.

Due Diligence Requirements:

- a. Standard CDD with additional verification where required;
- b. Verification of source of funds/business activity;
- c. Enhanced transaction monitoring;
- d. Periodic KYC updation every 8 years or as prescribed.

C. High Risk Customers

Customers posing higher AML/CFT risk due to customer profile, geography, business activity or transaction patterns shall be categorised as High Risk.

Illustrative categories:

- a. Politically Exposed Persons (“PEPs”);
- b. Non-resident customers from high-risk jurisdictions;
- c. Trusts, NGOs and charitable organisations;
- d. Customers dealing in cash-intensive businesses;
- e. Complex corporate structures with multiple layers;
- f. Customers with adverse media reports;
- g. Customers involved in virtual assets or high-risk industries;
- h. Non-face-to-face onboarding with insufficient verification;
- i. Customers flagged through sanctions/watchlists.

Enhanced Due Diligence (“EDD”) Requirements:

- a. Senior management approval before onboarding;
- b. Additional verification of identity and beneficial ownership;
- c. Verification of source of wealth and source of funds;
- d. Continuous monitoring of transactions;
- e. More frequent KYC updation;
- f. Review of customer relationship at least annually including risk reward analysis.

9.3 Risk Review and Reclassification

- 1. Customer risk categorization shall be reviewed periodically based on transaction behaviour and updated information.
- 2. Risk category may be upgraded or downgraded depending on the customer’s conduct and transaction profile.
- 3. High-risk accounts shall be subjected to enhanced scrutiny and monitoring.
- 4. The Compliance Officer shall maintain records of risk categorization and periodic review.

10. AADHAAR LINKED MOBILE NUMBER CHANGE MANAGEMENT

- a. The borrower shall ensure that the Aadhaar-linked mobile number registered with the Company remains active and updated at all times.
- b. Any change in the Aadhaar-linked mobile number shall be immediately communicated by the Company.
- c. Upon verification of such change, the Company may at its discretion assign a new Member Code/Customer ID.
- d. Existing loan accounts and outstanding balances may be migrated to the new Member Code after due verification and system validation.
- e. Failure to update Aadhaar-linked mobile number may result in restriction of digital access, transaction alerts or servicing requests.

11 . MONITORING AND REPORTING OF TRANSACTIONS

The Company shall monitor customer transactions on an ongoing basis considering the customer's risk profile.

The Company shall:

- a. Identify unusual, suspicious or inconsistent transactions.
- b. Monitor complex and unusually large transactions.
- c. Monitor transactions lacking apparent economic or lawful purpose.
- d. Conduct enhanced scrutiny for high-risk accounts.
- e. Validate customers against sanctions lists, RBI caution lists and public watchlists.
- f. File Suspicious Transaction Reports ("STRs") and other applicable reports with FIU-IND.

Special attention shall be paid to:

- a. Frequent cash transactions;
- b. Structuring/smurfing activities;
- c. Sudden repayment from unrelated third parties;
- d. Layered transactions;
- e. Transactions inconsistent with customer profile.

12. ENHANCED DUE DILIGENCE ("EDD")

EDD measures shall be undertaken for high-risk customers and transactions.

EDD may include:

- a. Additional identity verification;
- b. Video verification or physical verification;
- c. Verification of sources of funds and wealth;
- d. Obtaining audited financials and tax returns;
- e. Senior management approval;
- f. Enhanced monitoring frequency.

13. ONGOING DUE DILIGENCE

The Company shall conduct ongoing due diligence throughout the business relationship.

This includes:

- a. Periodic updation of KYC records;
- b. Monitoring transaction behaviour;
- c. Reviewing customer risk categorisation;
- d. Updating beneficial ownership details;
- e. Verifying continued legitimacy of business activity.

14. RISK MANAGEMENT

The Company shall implement an effective AML/CFT risk management framework including:

- a. Internal controls and compliance systems;
- b. Segregation of duties;
- c. Periodic internal audits;
- d. Independent compliance review;
- e. Employee training and awareness;
- f. Monitoring systems for suspicious transactions;
- g. Board oversight on AML compliance.

The Audit Committee/Board shall periodically review compliance with AML/KYC requirements

15. CUSTOMER EDUCATION

The Company shall educate customers regarding:

- a. Importance of KYC compliance;
- b. Requirement of document collection;
- c. Updating customer information;
- d. Prevention of identity theft and fraud;
- e. Reporting suspicious activity.

The Company may provide customer awareness materials through brochures, digital communication, website disclosures and branch interactions.

16. EMPLOYEE TRAINING

- a. The Company shall implement periodic AML/KYC training programs for employees.
- b. Frontline, operations, compliance and risk personnel shall receive role-based training.
- c. Employees shall be trained to identify suspicious transactions and escalation procedures.

17. APPOINTMENT OF PRINCIPAL OFFICER

The Company shall appoint a Principal Officer for AML/KYC compliance.

The Principal Officer shall:

- a. Monitor compliance with AML/KYC requirements;
- b. Report suspicious transactions to FIU-IND;
- c. Liaise with regulators and enforcement authorities;
- d. Maintain confidentiality of STR reporting;
- e. Ensure implementation of AML systems and controls;
- f. Submit regulatory reports within prescribed timelines.

The Principal Officer shall have direct access to the Board or designated committee.

18. MAINTENANCE OF RECORDS

The Company shall maintain records relating to:

- a. Customer identification documents;
- b. Account files and business correspondence;
- c. Transaction records;
- d. Suspicious transaction reports;
- e. Cash transaction reports;
- f. Risk categorization records.

Records shall be preserved for a minimum period of ten (10) years from the cessation of customer relationship or as prescribed under applicable law.

19. INFORMATION TO BE PRESERVED

The following information shall be preserved:

- a. Nature of transaction;
- b. Amount and currency of transaction;
- c. Date of transaction;
- d. Parties involved in the transaction;
- e. Supporting documents and communication.

20. REPORTING TO FINANCIAL INTELLIGENT UNIT-INDIA (“FIU-IND”)

The Company shall report the following transactions to FIU-IND within prescribed timelines:

- a. Cash Transaction Reports (“CTR”);
- b. Suspicious Transaction Reports (“STR”);
- c. Counterfeit Currency Reports;
- d. Other reports mandated under PMLA.

The Company and its employees shall maintain strict confidentiality regarding reporting of suspicious transactions.

21. DATA CONFIDENTIALITY AND SECURITY

- a. Customer information shall be maintained confidentially.
- b. Access to customer data shall be restricted to authorised personnel.
- c. Digital records shall be protected through appropriate cybersecurity controls.
- d. Customer information shall be shared only with customer consent in writing except where required by law or regulatory authorities.

22. POLICY REVIEW

- a. This Policy shall be reviewed periodically and updated in line with regulatory changes.
- b. The Board of Directors shall have authority to approve amendments to this Policy.
- c. Any changes in RBI/PMLA regulations shall automatically apply to the extent required.

23. BOARD APPROVAL

This AML and KYC Policy was approved by the Board of Directors on 20-03-2026.