

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

FRAUD RISK MANAGEMENT AND FRAUD PREVENTION POLICY

Board Approval Date: 20.03.2026

Sl No	INDEX	Page
1	PREAMBLE	2
2	OBJECTIVES	2
3	APPLICABILITY	2
4	FRAUD RISK GOVERNANCE STRUCTURE	3
5	DEFINITION OF FRAUD	3
6	FRAUD CLASSIFICATION	3
7	FRAUD RISK MANAGEMENT FRAMEWORK	4
8	EARLY WARNING SIGNALS (EWS)	5
9	FRAUD REPORTING MECHANISM	5
10	FRAUD INVESTIGATION PROCESS	6
11	FRAUD REGISTER	6
12	CUSTOMER FRAUD PREVENTION	7
13	DIGITAL AND CYBER FRAUD CONTROLS	7
14	BUSINESS CORRESPONDENT AND RECOVERY AGENT FRAUD CONTROLS	7
15	EMPLOYEE ACCOUNTABILITY	7
16	ROOT CAUSE ANALYSIS	7
17	TRAINING AND AWARENESS	8
18	REPORTING TO BOARD	8
19	CONFIDENTIALITY	8
20	POLICY REVIEW	8
21	BOARD APPROVAL	8

1. PREAMBLE

Lakme Investment and Finance Limited recognizes that fraud risk is a significant operational, financial, legal and reputational risk.

This Policy establishes a comprehensive framework for prevention, detection, reporting, investigation, monitoring and mitigation of fraud risks in accordance with:

- a. RBI Scale Based Regulation Framework;
- b. RBI Master Direction – Non-Banking Financial Company, as amended from time to time;
- c. RBI KYC Directions;
- d. Prevention of Money Laundering Act, 2002;
- e. RBI Digital Lending Guidelines;
- f. RBI Cyber Security and Information Technology Governance requirements;
- g. Companies Act, 2013;
- h. Applicable RBI circulars and regulatory instructions.

2. OBJECTIVES

The objectives of this Policy are:

- a. Prevent fraud through robust internal controls.
- b. Detect frauds at the earliest possible stage.
- c. Ensure timely investigation and reporting.
- d. Minimize financial losses.
- e. Protect customer interests.
- f. Strengthen fraud awareness among employees.
- g. Promote a zero-tolerance approach towards fraud.

3. APPLICABILITY

This Policy shall apply to:

- a. Directors;
- b. Employees;
- c. Key Managerial Personnel;
- d. Recovery Agents;
- e. Business Correspondents;
- f. Outsourcing Service Providers;
- g. Vendors;
- h. Consultants;
- i. Customers;
- j. Borrowers;
- k. Third-party service providers.

4. FRAUD RISK GOVERNANCE STRUCTURE

Board of Directors

The Board shall:

- a. Approve the Fraud Risk Management Policy.
- b. Review significant fraud cases.
- c. Monitor fraud trends and corrective actions.
- d. Put in place appropriate fraud prevention systems.

Risk Management Committee

The Committee shall:

- a. Monitor fraud risk indicators.
- b. Review fraud risk assessments.
- c. Evaluate fraud trends.

Recommend preventive actions.

Compliance Officer

The Compliance Officer shall:

- a. Maintain Fraud Register.
- b. Coordinate investigations.
- c. Monitor regulatory reporting.
- d. Submit reports to management and Board.

5. DEFINITION OF FRAUD

Fraud means any intentional act, omission, misrepresentation, concealment, forgery, manipulation, unauthorized activity or abuse of position resulting in wrongful gain to any person or wrongful loss to the Company, customer or stakeholder.

6. FRAUD CLASSIFICATION

A. Employee Fraud

Including:

- a. Misappropriation of funds;
- b. Unauthorized transactions;
- c. Fictitious accounts;
- d. Collusion with borrowers;
- e. Manipulation of records;
- f. Bribery and corruption.

B. Customer Fraud

Including:

- a. Forged documents;
- b. Identity fraud;
- c. Multiple financing fraud;
- d. Fake collateral;
- e. Misrepresentation of financial information.

C. Vendor and Outsourcing Fraud

Including:

- a. False invoices;
- b. Overbilling;
- c. Kickbacks;
- d. Service provider collusion;
- e. Recovery agent misconduct.

D. Cyber and Digital Fraud

Including:

- a. Phishing;
- b. Account takeover;
- c. Malware attacks;
- d. Unauthorized system access;
- e. Data theft;
- f. Digital lending fraud.

7. FRAUD RISK MANAGEMENT FRAMEWORK

The Company shall establish:

Preventive Controls

- a. Segregation of duties;
- b. Maker-checker controls;
- c. Dual authorization controls;
- d. Access management;
- e. Vendor due diligence;
- f. Employee background verification;
- g. Borrower verification.

Detective Controls

- a. Internal audit reviews;
- b. Surprise inspections;
- c. Transaction monitoring;
- d. Auto generated exception reports;
- e. Data analytics;
- f. Fraud alerts.
- g. Ethical hacking with Board approval to test resilience of the system

Corrective Controls

- a. Investigation;
- b. Recovery actions;
- c. Disciplinary proceedings;
- d. Legal action;
- e. Process improvements.

8. EARLY WARNING SIGNALS (EWS)

The following shall be treated as fraud indicators:

Borrower Related

- a. Frequent address changes;
- b. Forged KYC documents;
- c. Multiple loan applications;
- d. Sudden delays/deterioration in repayment.

Employee Related

- a. Override of controls;
- b. Unusual transactions;
- c. Frequent customer complaints;
- d. Reluctance/Refusal to take leave.

Vendor Related

- a. Abnormal billing patterns;
- b. Related party dealings;
- c. Duplicate payments.

Technology Related

- a. Repeated login failures;
- b. Unauthorized access attempts;
- c. Data extraction activities.

9. FRAUD REPORTING MECHANISM

Any employee, customer or stakeholder may report suspected fraud through:

- a. Reporting Manager;
- b. Compliance Officer;
- c. Whistle Blower Mechanism;
- d. Audit Committee Chairperson;
- e. Dedicated Fraud Reporting Email.

Reports may be made confidentially.

Retaliation against whistle blowers shall not be permitted.

10. FRAUD INVESTIGATION PROCESS

Upon receipt of a complaint:

Stage 1 – Preliminary Assessment

Within 7 days:

- a. Assess credibility.
- b. Preserve evidence.
- c. Determine severity.

Stage 2 – Investigation

Investigation Team may:

- a. Review records;
- b. Examine transactions;
- c. Conduct interviews;
- d. Analyse electronic evidence;
- e. Obtain legal opinion.

Stage 3 – Investigation Report

The report shall contain:

- a. Facts established;
- b. Persons involved;
- c. Financial impact;
- d. Control failures;
- e. Recommended actions.

11. FRAUD REGISTER

The Company shall maintain a Fraud Register containing:

- a. Fraud Reference Number;
- b. Date of Detection;
- c. Nature of Fraud;
- d. Amount Involved;
- e. Persons Involved;
- f. Investigation Status;
- g. Recovery Status;
- h. Closure Date.

Records shall be preserved for at least eight years.

12. CUSTOMER FRAUD PREVENTION

The Company shall implement:

- a. KYC verification;
- b. CKYC validation;
- c. PAN verification;
- d. Aadhaar authentication where permitted;
- e. Credit bureau verification;
- f. Property due diligence;
- g. Bank account validation.

13. DIGITAL AND CYBER FRAUD CONTROLS

The Company shall establish:

- a. Multi-factor authentication;
- b. User access controls;
- c. System audit trails;
- d. Cyber security monitoring;
- e. Data loss prevention controls;
- f. Incident response procedures.

14. BUSINESS CORRESPONDENT AND RECOVERY AGENT FRAUD CONTROLS

The Company shall:

- a. Conduct due diligence before appointment.
- b. Perform periodic reviews.
- c. Monitor field activities.
- d. Investigate customer complaints.
- e. Terminate engagements in case of fraud.

15. EMPLOYEE ACCOUNTABILITY

Employees involved in fraud may face:

- a. Suspension;
- b. Termination;
- c. Recovery proceedings;
- d. Civil action;
- e. Criminal prosecution.

Disciplinary action shall be based on investigation findings.

16. ROOT CAUSE ANALYSIS

Every confirmed fraud shall undergo Root Cause Analysis covering:

- a. Process failure;
- b. Control weakness;
- c. Technology weakness;
- d. Human error;
- e. Governance failure.

Corrective Action Plans shall be implemented.

17. TRAINING AND AWARENESS

Annual fraud awareness training shall be conducted covering:

- a. Fraud indicators;
- b. Cyber fraud;
- c. Customer fraud;
- d. Whistle blower reporting;
- e. Regulatory expectations.

18. REPORTING TO BOARD

Quarterly fraud reports shall be submitted to:

- a. Risk Management Committee;
- b. Audit Committee;
- c. Board of Directors.

The report shall include:

- a. Number of frauds detected;
- b. Amount involved;
- c. Recoveries made;
- d. Investigations pending;
- e. Corrective actions taken.

19. CONFIDENTIALITY

All fraud investigations shall be treated as confidential.

Information shall be shared strictly on a need-to-know basis.

20. POLICY REVIEW

This Policy shall be reviewed annually or earlier upon:

- a. Regulatory changes;
- b. Significant fraud incidents;
- c. Audit observations;
- d. Board directions.

Any amendment shall require approval of the Board.

21. BOARD APPROVAL

This Policy shall come into effect from the date approved by the Board of Directors of Lakme Investment and Finance Limited.