FRAUD MONITORING & REPORTING POLICY

(For Base Layer NBFC – Investment and Credit Company)

1. Objective

This Policy aims to:

- Establish a robust framework for *the* prevention, early detection, investigation, monitoring, and reporting of frauds.
- Ensure *strict* compliance with applicable provisions of the Reserve Bank of India ("RBI"), *the Companies Act, 2013, the Prevention of Money Laundering Act, 2002 (PMLA),* and other statutory authorities.
- Safeguard the Company's assets, reputation, customers, and stakeholder interests.
- Define clear internal reporting lines and *mandated* regulatory reporting procedures.
- Promote an ethical *corporate* culture with *absolute* zero tolerance towards fraud.

2. Scope

This Policy applies to:

- All employees (permanent, contractual, temporary, *and probationers*).
- Directors and Key Managerial Personnel *(KMP).*
- Vendors, service providers, agents, business correspondents, *Lending Service Providers (LSPs), and Co-lending partners*.
- Customers and third parties interacting with the Company.

It covers:

- Internal and external fraud.
- Attempted fraud and suspected fraud.
- Cyber fraud, technology-enabled fraud, *and digital payment gateway frauds*.
- Loan-related, operational, financial, and documentation fraud.
- Regulatory reporting obligations.

3. Regulatory Framework

This Policy is framed in accordance with:

- RBI Master Directions – Fraud Risk Management in NBFCs (as updated from time to time).
- RBI Master Direction – Non-Banking Financial Company – Scale Based Regulation (SBR).
- RBI Master Directions – Monitoring of Frauds in NBFCs.
- *Section 143(12) and Section 177 of the* Companies Act, 2013, *read with relevant rules regarding Vigil Mechanism and Auditor reporting*.
- *Prevention of Money Laundering Act, 2002 (PMLA) and the Information Technology Act, 2000.*
- Prevention of Corruption Act, 1988 *and applicable provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS).*
- Any other applicable RBI circulars, notifications, or guidelines issued from time to time.

4. Definitions

4.1 Fraud

Fraud includes any act, omission, concealment, manipulation, or misrepresentation committed intentionally to deceive, resulting in financial loss, wrongful gain, or reputational damage. *(This aligns with the broad definition provided under the Explanation to Section 447 of the Companies Act, 2013).*
Illustratively, fraud includes:

- Misappropriation of funds *and criminal breach of trust.*
- Forgery and falsification of *financial or operational* records.
- Fraudulent loan documentation *and identity theft (including synthetic identity fraud).*

- Bribery and corruption.
- Cyber fraud *(e.g., phishing, ransomware, account takeover)*.
- Unauthorized transactions *and UPI/Digital lending frauds*.
- Diversion or siphoning of funds.

4.2 Fraudulent Transaction

Any transaction executed with dishonest intent for wrongful gain or to cause loss, whether through manual manipulation or technological means, *including the circumvention of established internal controls*.

5. Fraud risk governance structure

5.1 Board of Directors *(and Audit Committee)*

The Board *(assisted by the Audit Committee, if applicable under Section 177 of the Companies Act)* shall:

- Oversee the effectiveness of the fraud risk management framework.
- Review fraud cases, *Root Cause Analyses (RCA)*, and status reports periodically.
- Ensure adequate internal control systems *are operationalized*.
- Approve this Policy and its amendments.

5.2 Fraud Monitoring Committee (FMC)

The Company shall constitute a Fraud Monitoring Committee comprising:

- Managing Director
- Chief Financial Officer
- Chief Risk Officer
- Compliance Officer
- Any other senior official as may be nominated *by the Board*

The FMC shall:

- Review fraud investigations and findings.
- Classify frauds as per RBI guidelines.
- Approve regulatory reporting *and disclosures*.
- Monitor corrective and preventive actions *(CAPA)*.

5.3 Fraud Investigation Unit (FIU)

The Company shall designate a Fraud Investigation Unit responsible for:

- Conducting detailed investigations of suspected or detected fraud.
- Preserving *digital and physical* evidence *in a forensically sound manner*.
- Coordinating with *Internal and Statutory* auditors and regulators.
- Ensuring timely reporting to RBI and law enforcement agencies.

The FIU shall report *directly* to the FMC.

6. Fraud risk management framework

6.1 Preventive Controls

The Company shall implement:

- Segregation of duties *and mandatory leave policies for sensitive positions*.
- Maker-checker mechanism *for all financial transactions*.
- Access controls, *Multi-Factor Authentication (MFA)*, and IT security protocols.
- *Comprehensive* employee *and promoter* background verification.
- Vendor due diligence *and right-to-audit clauses*.
- Periodic fraud awareness training.
- Data analytics and transaction monitoring systems.

6.2 Detection Controls

The Company shall adopt:

- Periodic internal audits *and concurrent audits.*
- Risk-based branch inspections *and* surprise checks.
- Exception reporting systems.
- Early warning signals (EWS) framework *to track portfolio health*.
- Whistleblower mechanism.
- Automated fraud detection tools *and Suspicious Transaction Reporting (STR) under PMLA.*

6.3 Corrective Controls

Upon detection of fraud:

- Immediate containment action *to freeze compromised accounts/systems*.
- Root cause analysis *(RCA)*.
- Strengthening of internal controls *to plug identified loopholes*.
- *Strict* disciplinary action *including termination*.
- Recovery proceedings *under applicable civil laws*.
- Legal action where required *(including filing of FIRs).*

7. Reporting of fraud

7.1 Internal Reporting

- All employees must immediately report suspected fraud to *the* FIU.
- *The* FIU shall place findings before *the* FMC.
- A centralized fraud register shall be maintained *and updated concurrently*.
- *Statutory Auditors must be informed immediately if the suspected fraud amount is ₹1 crore or above, to enable them to fulfill their reporting obligations to the Central Government under Section 143(12) of the Companies Act, 2013.*

7.2 Reporting to RBI

Frauds shall be reported as per *the latest* RBI guidelines *(via the RBI's XBRL/APEX portal)*:

- **Frauds of ₹1 crore and above:** To be reported in *the* prescribed format (FMR-1) within 3 weeks of detection.
- **Frauds below ₹1 crore:** To be reported on a quarterly basis.
- **Frauds of ₹50 lakh and above:** Detailed case-specific reports including root cause and preventive measures *must be submitted*.
- *All frauds, regardless of the amount, shall be updated in the Central Fraud Registry (CFR) as per regulatory mandates.*
- All reporting shall be strictly in accordance with RBI Master Directions.

7.3 Reporting to Law Enforcement Agencies

Depending on *the* nature of *the* fraud, cases may be reported to:

- Economic Offences Wing (EOW)
- Cyber Crime Cell
- Local Police Authorities *(via filing of an FIR under the Bharatiya Nyaya Sanhita, 2023)*
- Any other competent authority *(e.g., Enforcement Directorate, if money laundering is suspected).*
  The Company shall extend full cooperation during *any state or central* investigation.

8. Escalation matrix

- Branch Level → Fraud Liaison Officer (FLO) → FIU → FMC → Board *(or Audit Committee).*
- Any fraud involving senior management, significant financial exposure, or reputational risk shall be immediately escalated to the Board.

9. Whistleblower mechanism

In compliance with Section 177(9) of the Companies Act, 2013 and Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014, the Company shall maintain a *Vigil/Whistleblower* Policy ensuring:

- Confidential reporting channels (email, hotline, *dedicated web* portal).
- *Absolute* protection against retaliation *or victimization of the whistleblower*.

- Direct access to *the Chairperson of the* Audit Committee / Board in appropriate *or exceptional* cases. Details shall be *prominently* displayed at *all* branches and *on the Company's* website.

10. Roles & responsibilities

Authority	Responsibility
Board	Overall supervision, periodic review, *and setting the "Tone at the Top"*.
FMC	Monitoring, classification, regulatory reporting, *and CAPA enforcement*.
FIU	Investigation, documentation, *and evidence preservation*.
Employees	Mandatory reporting of suspicious activities and *strict* adherence to controls.

11. Review of policy

This Policy shall be:

- Reviewed annually; or
- Earlier, if required due to regulatory changes, operational developments, *or amendments to the Companies Act/RBI Master Directions*.
  Amendments shall require *formal* Board approval.

12. Zero tolerance statement

THIRUKOCHI FINCAP LIMITED maintains a *strict* zero-tolerance approach towards fraud, corruption, and unethical conduct. Any violation shall attract strict disciplinary and legal action, *including civil recovery and criminal prosecution*.

13. Effective date and approval

This **FRAUD MONITORING & REPORTING POLICY** has been approved by the Board of Directors of **THIRUKOCHI FINCAP LIMITED** at its meeting held on **12/03/2026**.

Effective Date: 12/03/2026

Version:1