

KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING (AML) POLICY

(For Base Layer NBFC – Investment and Credit Company)

1. Preamble

This Policy is framed in accordance with:

- KYC Master Direction, 2016 issued by the Reserve Bank of India (*as amended up to 2025/2026*)
- Scale Based Regulation (SBR) Framework for NBFCs
- Prevention of Money Laundering Act, 2002 (PMLA) *and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules), including recent amendments*
- Directions and circulars issued by RBI from time to time
- *The Unlawful Activities (Prevention) Act, 1967 (UAPA)*
- *The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act)*
- *The Digital Personal Data Protection (DPDP) Act, 2023*
- Money laundering refers to any activity connected with proceeds of crime including concealment, possession, acquisition or use and projecting it as untainted property.

The Company is committed to:

- ✓ Prevent misuse of its financial channels
- ✓ Detect and report suspicious transactions *to the Financial Intelligence Unit - India (FIU-IND)*
- ✓ Comply with regulatory obligations
- ✓ Maintain integrity and transparency in operations *while ensuring the protection of customer data*

2. Objectives of the policy

This Policy aims to:

1. Establish robust Customer Due Diligence (CDD) procedures
2. Prevent money laundering and terrorist financing
3. Define a risk-based customer acceptance framework
4. Ensure timely reporting of suspicious transactions
5. Protect the Company from reputational and regulatory risk
6. Create an AML compliance culture across the organization
7. *Establish a framework for periodic updation of KYC (Re-KYC) and screening against statutory sanction lists.*

3. Applicability

This Policy applies to:

- All branches and Head Office
- All employees, officers and management
- All products including gold loans, business loans, property loans and term loans
- Third-party relationships, outsourcing arrangements, *Lending Service Providers (LSPs), and Digital Lending Applications (DLAs) operating on behalf of the Company*

Non-compliance shall attract disciplinary action *and potential statutory penalties.*

4. Key definitions

Important definitions under this policy align with:

- Prevention of Money Laundering Act, 2002 *and PML Rules*
- RBI Master Directions

Key terms include:

- Customer – Person engaged in a financial transaction with the Company
- Suspicious Transaction – Transaction lacking economic rationale, *involving unexplained large cash amounts*, or linked to crime/terror financing
- Proceeds of Crime – Property derived from criminal activity
- Politically Exposed Person (PEP) – Individual entrusted with a prominent public function in a foreign country *or domestically (as per FATF guidelines)*
- Principal Officer – Officer designated for STR/CTR reporting to *FIU-IND*
- **Beneficial Owner (BO)** – *The natural person who ultimately owns or controls a client and/or the person on whose behalf a transaction is being conducted.*

5. Governance structure

5.1 Board of Directors

The Board shall, *in alignment with its risk management obligations under Section 134 of the Companies Act, 2013*:

- Approve *the* KYC & AML Policy
- Review AML compliance periodically
- Ensure adequate systems & controls
- Monitor STR/CTR reporting trends
- **Ensure that the policy does not result in the denial of financial services to the financially/socially disadvantaged (financial inclusion).**

5.2 Principal Officer (PMLA)

The Company shall appoint a Principal Officer (*at management level*) responsible for:

- Monitoring suspicious transactions
- Filing STR with FIU-IND within *the* prescribed timeline (*within 7 days of arriving at a conclusion*)
- Coordinating with regulators *and law enforcement agencies*
- Maintaining AML records

5.3 Designated Director

A Designated Director shall ensure overall compliance under PMLA. *As per PML Rules, this person must hold the position of Managing Director or a whole-time Director, and shall not be the same person as the Principal Officer.*

6. Four core elements of KYC framework

- 1 Customer Acceptance Policy (CAP)
- 2 Customer Identification Procedures (CIP)
- 3 Risk Classification & Risk Management
- 4 Ongoing Monitoring & Reporting

7. Customer acceptance policy (cap)

The Company shall ensure:

- No anonymous or fictitious accounts
- No benami transactions
- No relationship with sanctioned individuals/entities (*Screening against UAPA and ISIL/Al-Qaida sanctions lists before onboarding and continuously thereafter*)
- Risk categorization at *the* onboarding stage
- **Mandatory upload of KYC data to the Central KYC Records Registry (CKYCR) within 10 days of commencement of an account-based relationship.**

7.1 Risk Categorization

Customers shall be classified as:

- Low Risk
- Medium Risk
- High Risk

Risk classification shall consider:

- Nature of business
- Geography
- Source of funds
- Transaction pattern
- Occupation

High-risk customers require enhanced due diligence.

7.2 Prohibited Categories

- The Company shall avoid lending to: Blacklisted borrowers
- Persons involved in financial fraud
- Individuals previously identified for spurious gold pledging
- Sanctioned individuals/entities
- Shell entities (*companies incorporated with no significant operations or assets*)

8. Customer identification procedure (CIP)

Customer identity shall be verified through:

- Officially Valid Documents (OVD) *such as Passport, Driving License, Voter ID, NREGA Job Card, or letter issued by the National Population Register.*
- Aadhaar (voluntary and as per law, *using offline verification or OTP-based e-KYC subject to explicit consent*)
- PAN (mandatory in specified thresholds *under Rule 114B of the Income Tax Rules, 1962*)
- *Video based Customer Identification Process (V-CIP) (where implemented by the Company in compliance with RBI technical specifications).*

Identity verification shall include:

- ✓ Original document verification
- ✓ Certified copy marking (*or digital equivalent like DigiLocker verification*)
- ✓ Photograph
- ✓ Address verification
- ✓ Contact details

Re-KYC shall be done periodically based on risk category:

- *High Risk: Once every 2 years*
- *Medium Risk: Once every 8 years*
- *Low Risk: Once every 10 years*

9. Individual customer documentation

9.1 Gold Loans

Mandatory:

- Aadhaar (*Voluntary/Offline XML*) / OVD
- PAN (for aggregate *exposure of ₹5 lakh and above, or cash transactions as per IT Rules*)
- Additional address proof if required.

9.2 Business / Property Loans

- PAN (Mandatory irrespective of amount)
- ID proof of applicant & guarantor
- Bank statements (minimum 6 months)
- Property tax receipt
- Registration documents (if applicable)

9.3 Term Loans

- PAN (Mandatory for ₹50,000 and above)
- ID proof
- Bank statements

10. Non-individual customer due diligence

10.1 Companies

Documents required:

- Certificate of Incorporation
- MOA & AOA
- Board Resolution
- PAN
- List of Directors

Beneficial ownership identification is mandatory. *As per recent PMLA amendments, the threshold for determining controlling ownership interest in a company is now 10% of shares, capital, or profits.*

10.2 Partnership Firms

- Registration certificate
- Partnership deed
- PAN
- Authorization letter
- KYC of authorized signatory

Beneficial ownership threshold for partnerships is 15% of capital or profits.

10.3 Trusts

- Registration certificate
- Trust deed
- PAN / Form 60
- Resolution
- KYC of trustees & authorized signatory
- *Beneficial ownership threshold for trusts is 10% of interest in the trust.*

10.4 Beneficial Ownership

The Company shall identify:

- Natural persons controlling \geq prescribed percentage (*10% for companies/trusts, 15% for partnerships/unincorporated bodies*)
- Persons exercising control *through voting rights or management.*

11. Enhanced due diligence (EDD)

EDD shall apply to:

- High-value transactions
- High-risk customers
- PEPs
- Customers from high-risk jurisdictions (*as identified by FATF*)
- Complex or unusual transactions

EDD measures include:

- Source of funds verification

- Senior management approval
- Increased monitoring frequency
- Additional documentation
- ***Compliance with Section 12AA of the PMLA prior to commencement of specific transactions.***

12. Politically exposed persons (peps)

Accounts of PEPs shall require:

- Senior management approval
- Source of wealth verification
- Ongoing enhanced monitoring

Relationship shall be reviewed periodically. *(Family members and close relatives of PEPs shall also be subjected to similar EDD measures).*

13. Ongoing monitoring

13.1 Threshold Monitoring

- Transactions above ₹50,000 – due diligence ***and PAN/Form 60 requirement***
- Ongoing due diligence mandatory above ₹1,00,000
- PAN mandatory for ₹5 lakh and above ***aggregate exposures***
- High-risk accounts shall be closely monitored.

13.2 Suspicious Transaction Monitoring

Red flags include:

- Structuring transactions to avoid reporting (***Smurfing***)
- Frequent cash dealings
- Fake documentation
- Sudden surge in activity
- Counterfeit currency
- Third-party payments without reason
- ***Reluctance to provide KYC documents or providing forged documents.***

14. Reporting obligations

14.1 STR (Suspicious Transaction Report)

Filed with FIU-IND ***via the FINnet 2.0 portal*** within the prescribed timeline ***(no later than 7 days from the date of arriving at a conclusion that the transaction is suspicious).***

Customer shall NOT be informed (no tipping off).

14.2 CTR (Cash Transaction Report)

Filed as per regulatory requirements ***(for cash transactions exceeding ₹10 lakhs, or series of integrally connected cash transactions exceeding ₹10 lakhs in a month).*** ***To be filed by the 15th day of the succeeding month.***

14.3 Record Maintenance

Records shall be maintained for:

- Minimum 5 years from transaction date
- 5 years after relationship termination
- ***Records must be maintained in a manner that allows swift reconstruction of individual transactions (including amounts and currencies involved) for FIU-IND or law enforcement.***

15. AML initiatives

The Company shall implement:

- ✓ Employee training programs (annual)
- ✓ Internal audit of AML compliance
- ✓ Risk-based monitoring systems

- ✓ Segregation of duties
- ✓ AML awareness culture
- ✓ **Robust IT systems to scan customer profiles against domestic and international sanction lists.**

16. Role of internal audit

Internal Audit shall:

- Review KYC documentation
- Test STR reporting system
- Evaluate compliance effectiveness
- Suggest improvements

Serious lapses shall be escalated to the Board *and the Audit Committee*.

17. Third-party reliance

The Company may rely on due diligence by regulated entities, provided:

- Records obtained within 2 days (*updated per RBI norms*)
- Ultimate responsibility remains with *the Company*
- RBI outsourcing guidelines are followed
- ***The third party is regulated, supervised, and has measures in place for CDD and record-keeping.***

18. Counterfeit currency handling

Bulk counterfeit detection:

- Record immediately
- Escalate to Principal Officer
- Report as required (***Counterfeit Currency Report - CCR to FIU-IND by the 15th of the succeeding month, and FIR with local police as per RBI Master Circular on Detection of Fake Indian Currency Notes.***)

19. Confidentiality & data privacy

Customer information shall:

- Be used only for regulatory and business purposes
- Not be shared for cross-selling ***without explicit consent***
- Be disclosed only to regulators/credit bureaus as permitted
- ***Be processed strictly in compliance with the Digital Personal Data Protection (DPDP) Act, 2023, ensuring data minimization, purpose limitation, and secure storage.***

20. Training & awareness

- Mandatory AML training for all employees
- Induction training for new recruits
- Periodic refresher training
- Specialized training for branch managers ***and onboarding staff to identify red flags.***

21. Policy review

This Policy shall be:

- Reviewed annually
- Updated upon regulatory changes
- Approved by Board for amendments

22. Consequences of non-compliance

Failure to comply may result in:

- Regulatory penalties ***under PMLA and RBI Act***

- Disciplinary action
- Termination of employment
- Legal consequences under PMLA (*including imprisonment or attachment of property for involved individuals*)

23. Effective date

This **KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING (AML) 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

