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

OF

MEGHDOOT Mercantile PRIVATE LIMITED

1. Introduction

The Reserve Bank of India (RBI) has issued guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards, which mandate that all Non-Banking Financial Companies (NBFCs) formulate and adopt suitable policies with the approval of their Board of Directors. Meghdoot Mercantile Private Limited ("the Company" or "Meghdoot"), as a Regulated Entity, is obligated to comply with these directives.

This policy ("KYC-AML Policy" or "Policy") is framed in accordance with:

- The RBI Master Direction - Know Your Customer (KYC) Direction, 2016, as notified via DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, along with subsequent amendments or re-enactments.
- The Prevention of Money Laundering Act, 2002 ("Act" or "PMLA").
- The Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("Rules").
- Other relevant laws, regulations, and guidelines, including FATCA/CRS and CKYCR requirements.

The Board of Directors of Meghdoot Mercantile Private Limited ("Board") has approved this KYC-AML Policy. The primary objectives of this policy are to:

1. Identify and understand customers and their financial dealings effectively.
2. Manage risks prudently to ensure the integrity of the Company's operations.
3. Prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering, terrorist financing, or other unlawful activities.

2. Applicability

This Policy applies to all offices, branches, departments, employees, and authorized representatives of Meghdoot involved in dealing with customers and their financial transactions. It applies to the onboarding process of customers through various channels, including physical (face-to-face) interactions, digital/on-line platforms (mobile app and web-based platforms), and any outsourced or third-party arrangements related to customer identification and verification.

3. Definitions

For the purposes of this Policy, the following definitions apply:

- **Aadhaar number:** As defined in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (18 of 2016).
- **Authentication (Aadhaar):** The process defined under sub-section (c) of section 2 of the Aadhaar Act, involving verification of demographic and/or biometric data.
- **Customer:** A person who is engaged in a financial transaction or activity with the Company, and includes a person on whose behalf another is acting.
- **Act (PMLA) and Rules:** Refers to the Prevention of Money Laundering Act, 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, including all amendments and notifications issued thereunder.
- **Customer Due Diligence (CDD):** The process of identifying and verifying the customer's identity and, where applicable, the beneficial owner(s), and understanding the purpose and intended nature of the business relationship.

- **Central KYC Records Registry (CKYCR):** An entity defined under Rule 2(1)(aa) of the Rules to receive, store, safeguard and retrieve KYC records in digital form.

- **Digital KYC:** The process of capturing the live photo of the customer, along with scans/images of Officially Valid Documents (OVDs) or equivalent e-documents, the proof of possession of Aadhaar (where offline verification cannot be carried out), and the geo-coordinates (latitude and longitude) of the location where the photo is taken by an authorized officer. Digital KYC must be conducted as per provisions contained in the PMLA and applicable rules/directions.

- **Digital Signature:** Has the meaning assigned to it in clause (p) of sub-section (1) of Section 2 of the Information Technology Act, 2000 (21 of 2000).

- **Equivalent e-document:** An electronic equivalent of an OVD, issued by the document's issuing authority with a valid digital signature, including documents issued to the customer's digital locker account under the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

- **KYC Identifier (CKYCR number):** The unique number or code assigned by the Central KYC Records Registry to a customer.

- **Officially Valid Document (OVD):** Passport, driving license, proof of possession of Aadhaar (masked Aadhaar), Voter's Identity Card, job card issued by NREGA duly signed by a State Government officer, and letter issued by the National Population Register containing name and address details. In case Aadhaar is used as OVD, it may be submitted in such form as issued by the Unique Identification Authority of India (UIDAI).

- **Digital Platform:** The mobile application and/or web-based platform through which the Company provides personal loans and advances to customers.

- **Principal Officer (PO):** An officer nominated by the Company who shall be responsible for furnishing information under rule 8 of the Rules, reporting

suspicious transactions to FIU-IND, and ensuring overall compliance with the PMLA directives.

- **Transaction:** Includes a wide range of financial activities such as account opening, deposits, withdrawals, exchanges, transfers of funds (in any currency, through any instrument or electronic means), use of a safety deposit box, fiduciary relationships, payments made or received under contractual obligations, and formation of legal persons or arrangements.

- **Video-based Customer Identification Process (V-CIP):** A process where an authorized official of the Company undertakes seamless, secure, real-time, consent-based audio-visual interaction with the customer to obtain identification information, verify documents required for CDD, and ascertain the veracity of the information furnished by the customer. V-CIP is treated as a face-to-face process for the purpose of this Policy.

4. Elements of the KYC-AML Policy

The Company's KYC-AML Policy rests on the following four key elements:

1. **Customer Acceptance Policy (CAP)**
2. **Customer Identification Procedure (CIP)**
3. **Monitoring of Transactions**
4. **Risk Management**

5. Customer Acceptance Policy (CAP)

The Customer Acceptance Policy outlines the manner in which the Company will accept customers. Key aspects include:

- **No Anonymous or Fictitious Accounts:** The Company will not open accounts or disburse loans in anonymous, fictitious, or benami names, or if the identity of the customer cannot be verified.

- **Customer Identity Verification:** Customers will be accepted only after verifying their identities as per the CDD process. If adequate CDD cannot be carried out due to non-cooperation or unreliable information, the relationship will not be established.

- **Compliance with CDD for Transactions:** No transaction or account-based relationship will be commenced without following the prescribed CDD procedures.

- **Mandatory KYC Information:** The mandatory information required for KYC purposes must be collected at the time of account opening and updated periodically as mandated by regulations.

- **Optional Information:** Additional information beyond what is mandated may be collected only with the customer's explicit consent and not as a condition for opening the account.

- **Third-Party Representation:** Where a customer acts on behalf of another, clear guidelines will be implemented, ensuring compliance with applicable laws (e.g., accounts operated by mandates or intermediaries acting in fiduciary capacities).

- **Sanction List Screening:** The Company shall implement robust screening against sanctions lists circulated by the RBI or other regulatory/government authorities to ensure that no sanctioned individual or entity is onboarded.

- **Customer-Friendly Approach:** While ensuring compliance, the Company shall be mindful not to inconvenience genuine and bona fide customers, and will not deter or discriminate against financially or socially disadvantaged sections from accessing financial services.

6. Customer Identification Procedure (CIP) and Customer Due Diligence (CDD)

Customer Identification:

Customer Identification involves verifying the customer's identity based on reliable, independent documents, data, or information. The objective is to be fully satisfied that

the customer is who they claim to be. The Company shall collect sufficient information to understand the nature of the customer's activities and the purpose and intended nature of the relationship.

Customer Due Diligence (CDD) Procedure:

For establishing an account-based relationship, the Company shall obtain:

(A) Proof of Identity (POI)

- Scan/Image of the PAN card or the equivalent e-document thereof must be uploaded on the Company's Digital Platform at the time of onboarding. PAN serves as a crucial identity verification document.

(B) Proof of Address (POA)

- Scan/Image of any ONE of the following to be uploaded on the Digital Platform:

  1. Passport or the equivalent e-document thereof
  2. Voter Identity Card or the equivalent e-document thereof
  3. Masked UIDAI card (Aadhaar) or the equivalent e-document thereof containing details of identity and address

- **Address Mismatch Protocol:** If, during subsequent physical face-to-face KYC verification (triggered when the cumulative loan amount disbursed to a borrower in a financial year exceeds a certain threshold amount, as determined by the Company), it is found that the address mentioned in the submitted OVD does not match the current residence address of the customer, the customer must mandatorily provide a current resident address proof. Acceptable current address proofs include Rent Agreement, Utility Bills (Electricity, Telephone, Post-paid Mobile, Piped Gas, Water), or Municipal Tax Receipt.

(C) Real-Time Selfie

- Customers must capture a real-time selfie during the loan application process through the Company's mobile application. This ensures authenticity and prevents impersonation by verifying that the customer is present in real-time.

CDD Measures Based on Risk and Loan Amount:

- If the total borrowed amount by a single borrower, whether in one or multiple tranches, exceeds INR [____]/- in a financial year, the Company shall conduct enhanced CDD, which may include physical face-to-face verification or Video-based Customer Identification Process (V-CIP).

OTP-Based e-KYC:

- The Company may open accounts using OTP-based e-KYC in non-face-to-face mode, subject to conditions imposed by the RBI, such as:
  - Obtaining the customer's explicit consent for OTP-based authentication.
  - Restricting the aggregate amount of term loans sanctioned in a financial year when using OTP-based KYC to not exceed INR 60,000.
  - Obtaining the customer's declaration that no other account has been or will be opened using OTP-based KYC with the Company or another financial institution.
  - Marking such accounts as opened via OTP-based e-KYC in CKYCR and updating status upon completion of full CDD.

Video-based Customer Identification Process (V-CIP):

- The Company may undertake V-CIP for establishing account-based relationships, subject to:
  - Informed consent from the customer.
  - Verification of PAN and Aadhaar through offline methods, ensuring the generation date of the Aadhaar XML file/QR code is within three days of the V-CIP.

- Recording live video and capturing a clear image of the customer holding their PAN card (unless e-PAN is used).
- Geo-tagging the customer's location to ensure presence in India.
- Conducting real-time interactions with dynamic questioning to rule out pre-recorded sessions.
- Running a concurrent audit of the V-CIP process before activation of the account.
- Ensuring robust data security, encryption, and maintaining logs with credentials of the official conducting the interaction.

Redaction of Aadhaar Number:

- The Company must ensure compliance with Section 16 of relevant Aadhaar regulations and must redact/blackout the Aadhaar number in all records.

Use of Advanced Technologies:

- The Company is encouraged to leverage AI, facial recognition, and other advanced technologies to strengthen the integrity of the identification process. However, the ultimate responsibility for accurate CDD rests with the Company.

Unique Customer Identification Code (UCIC):

- A UCIC shall be assigned to every customer to help track multiple relationships and ensure that the customer's identity is consistently established across products and services.

7. Monitoring of Transactions

Ongoing Monitoring:

- Ongoing transaction monitoring is critical. Officials must understand the customer's typical transactional behavior to identify deviations that could indicate suspicious activities.

Unusual Transactions:

- Special attention should be given to large, complex, or unusual transactions that do not have an apparent lawful purpose. Transactions that appear inconsistent with the customer's known profile should trigger scrutiny.

Threshold Limits and Alerts:

- The Company may set internal threshold limits for transactions and scrutinize all transactions that exceed these limits. Cash transactions that are large and inconsistent with a customer's regular activity profile are red flags.

High-Risk Accounts:

- High-risk customer accounts will be subject to enhanced monitoring measures. The frequency and intensity of monitoring depend on the assessed risk category.

Periodic Risk Review:

- The Company shall periodically review and re-categorize customer risk profiles based on transactional patterns and relevant risk indicators. This helps ensure that enhanced due diligence measures are applied appropriately as the risk profile evolves.

8. Risk Management

Risk-Based Approach:

The Company adopts a risk-based approach (RBA) for assessing and managing money laundering (ML) and terrorist financing (TF) risks. Customers are broadly classified into Low, Medium, and High risk, considering factors such as:

- Credit evaluation and repayment history.
- Nature and location of customer's activities.
- Country of origin, sources of funds, and client characteristics.

- Volume, value, and pattern of transactions.

Annual Risk Assessment:

- The Company shall conduct an annual risk assessment for ML/TF and document the findings.
- The results will be presented to the Board of Directors or a delegated authority and made available to regulatory authorities upon request.
- Controls and procedures shall be periodically reviewed for efficacy, and improvements implemented as necessary.

9. Appointment of Principal Officer (PO)

Principal Officer Responsibilities:

- The Company shall appoint a Principal Officer at a senior management level who will:
    - Oversee the monitoring and reporting of all transactions.
    - Furnish requisite information to the Director of FIU-IND and relevant regulatory bodies.
    - Maintain liaison with enforcement agencies, other NBFCs, and financial institutions.

- The name, designation, and address of the PO shall be communicated to FIU-IND and/or RBI.

10. Reporting to Financial Intelligence Unit-India (FIU-IND)

Regulatory Reporting:

- Pursuant to Section 12 of the PMLA and Rule 3 of the Rules, the Company must report certain prescribed transactions (cash and suspicious) to the Director, FIU-IND.

- Information related to transactions mentioned in clause (A), (B), and (BA) of Sub-rule (1) of Rule 3 of the PML Rules must be submitted by the 15th of the succeeding month.
- Information on transactions described in clause (D) of Sub-rule (1) of Rule 3 (suspicious transactions) should be reported to FIU-IND within seven working days from the date of determining the suspicion.

Confidentiality and Non-Disclosure:

- The Company and its employees must maintain strict confidentiality regarding the fact of reporting and the contents of the reports.
- No "NIL" reports are required where no cash or suspicious transactions took place during a reporting period.

Delayed Reporting:

- Any delay or inaccuracy in reporting beyond the specified time limit is considered a separate contravention for each day of delay.

11. Appointment of Designated Director

Designated Director Responsibilities:

- The Board shall appoint a Designated Director to ensure compliance with AML/CFT obligations.
- The Designated Director should be in senior management or an equivalent position.

- The Principal Officer cannot be the Designated Director.
- The name, designation, and address of the Designated Director shall be communicated to FIU-IND.

12. Record Maintenance and Preservation

Record Retention:

- The Company is required to maintain records of all transactions referred to in Section 12(1)(a) of PMLA and Rule 3 of the Rules for a period of five years from the date of the transaction.
- Records of the identity and address of customers must be maintained for five years after the business relationship ends or the account is closed, whichever is later.
- Other records not related directly to identity or transactions must be retained for at least five years from the date of the record.

Destruction of Records:

- Each department shall maintain a destruction register under the custody of a senior management officer. The register shall include details of records destroyed and the approving officer's name and designation.

Data Accessibility and Security:

- The Company shall implement a robust system for maintaining both hard and soft copies of records, ensuring efficient retrieval upon request by regulatory authorities.
- Records shall be stored securely to prevent unauthorized access or tampering.

13. Compliance with CKYCR, FATCA/CRS Requirements

CKYCR Compliance:

- As per RBI directions, the Company shall upload KYC data to the Central KYC Records Registry (CKYCR) for all new individual accounts opened on or after November 1, 2016.
- The Company shall also maintain KYC data for existing customers in digital format and update loan application forms to align with RBI-prescribed templates.

FATCA/CRS Compliance:

- The Company shall ensure full compliance with the Common Reporting Standards (CRS) guidelines, as issued by RBI and the Government of India from time to time.

14. Money Laundering and Terrorist Financing (ML/TF) Risk Assessment

- The Company will conduct an annual ML/TF risk assessment and document the process, methodology, and findings.
- The results will be placed before the Board or delegated authorities and made available to regulatory or self-regulatory bodies upon request.
- A Risk-Based Approach (RBA) ensures that policies, controls, and procedures to manage and mitigate risks are approved by the Board and continuously monitored for effectiveness.

15. Reliance on Third-Party Due Diligence

- The Company may rely on third-party CDD if:
    - The third party provides necessary CDD information within seven days.
    - The Company obtains copies of identification data and other documents relating to the client's CDD upon request.
    - The third party is regulated, supervised, or monitored and adheres to record-keeping and CDD standards equivalent to the Company's.
    - The third party is not based in a high-risk country or jurisdiction.
- Despite reliance on third parties, ultimate responsibility for CDD and AML/CFT compliance rests with the Company.

16. Technology and Security Measures

- The Company will use secure, end-to-end encrypted platforms for digital KYC processes, ensuring no tampering or unauthorized access.
- Adequate software and security audits shall be conducted to maintain the integrity of the V-CIP and other e-KYC processes.

- The Company shall comply with data privacy laws and mask/redact sensitive information, such as Aadhaar numbers, to maintain confidentiality and customer privacy.

17. Training and Employee Awareness

- The Company shall conduct ongoing training programs for employees and authorized personnel to ensure they understand KYC/AML regulations, processes, and their role in detecting and preventing money laundering and terrorist financing.
- Training shall cover the identification of suspicious activities, regulatory changes, and the importance of adhering to the Policy.

18. Review of Policy

- This Policy shall be reviewed periodically (at least annually) or upon significant regulatory changes.
- Any changes or updates to the Policy shall be approved by the Board of Directors.
- The Company will ensure that the Policy remains current, comprehensive, and fully compliant with prevailing laws and regulatory expectations.

19. Effective Date

- This KYC-AML Policy is effective from the date of approval by the Board of Directors and shall remain in force until revised or superseded by a subsequent version.

20. Conclusion

This comprehensive KYC-AML Policy ensures that Meghdoot Mercantile Private Limited adheres to all applicable legal and regulatory requirements. By integrating rigorous customer identification measures, continuous transaction monitoring, robust risk management, and strict record-keeping and reporting obligations, the Policy safeguards

the Company's reputation, prevents misuse of its services, and promotes financial inclusion responsibly.

All employees, representatives, and officers of the Company are required to comply with this Policy. The ultimate responsibility for the implementation of the KYC-AML framework rests with the Board of Directors and senior management, who shall ensure that the Company's systems and processes remain effective, dynamic, and in alignment with regulatory expectations.

Approved by the Board of Directors of Meghdoot Mercantile Private Limited on 20th June, 2024.

For, MEGHDOOT MERCANTILE (P) LTD.

DIRECTOR