KYC AND AML POLICY OF MUTHOOTTU MINI FINANCIERS LIMITED

Reviewed and Approved in the Meeting of the Board of Directors held on 13/02/2023

In accordance with the Master Directions issued (as amended from time to time) by Reserve Bank of India, all Regulated Entities (REs) including Muthoottu Mini Financiers Limited (MMFL) is required to put in place appropriate Policy and procedures to comply with the relevant Know Your Customer (KYC) norms and Customer Due Diligence (CDD) processes at the time of onboarding the Customer and also during the continued relationship with such Customer which includes monitoring of transactions in terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India:

1. POLICY STATEMENT

MMFL is primarily engaged in Gold loan finance and by nature of its business operations, has low potential risks of money laundering, terrorist financing. MMFL understands the importance of the AML programs and commits itself to inculcating a vigilant culture in combating money laundering to the extent applicable to the Company. Accordingly, a KYC & AML Policy is prepared in line with RBI Directions and Prevention of the Money Laundering Act, 2002 rules as amended from time to time as well that of the norms put out by the other relevant regulations that is applicable to its business operations, for the time being in force.

2. OBJECTIVES OF THE POLICY:

The Policy seeks to achieve the
following objectives.

- To provide a framework for how the company, in its process of conducting business with Customers, will deal with the threat of money laundering and terrorism financing.
- To prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities

- That all the staff are aware and receive training on the Anti-Money laundering legislation applicable to them, as well as to adhere to their responsibilities under the regulations
- To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
- To enable the Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities as envisaged under the Prevention of Money Laundering Act, 2002 and in accordance with laid down procedures.
- To comply with applicable laws and regulatory guidelines

3. SCOPE OF THE POLICY

This Policy applies to all employees of MMFL and third-party agents engaged by it. The Policy seeks to maintain high standards of conduct within the Company and among its agents, if any, by preventing criminal activity through money laundering

The legislative requirements concerning anti-money laundering procedures are extensive and complex. This Policy aims to meet the legal requirements proportionate to the intensity of risks that MMFL is exposed to in respect of the businesses/activities (business verticals) being undertaken by the company as detailed below.

- Gold Loan including all types (online or offline)
- Remittances
- Depository Participant
- Money Changing
- Microfinance

4. IMPORTANT DEFINITIONS

i. “Central KYC Records Registry” (CKYCR) means an entity defined under Rule 2(1) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to receive ,store, safeguard and retrieve the KYC records in digital form of a Customer.

ii. “Customer “means.

A. person who is engaged in a financial transaction or activity with MMFL and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.

B. any other person connected with a financial transaction which can pose significant reputation or other risks to MMFL.

iii. "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

iv. Know Your Client (KYC) Identifier" means the unique number or code assigned to a Customer by the Central KYC Records Registry.

v. Non-face-to-face Customers means Customers who open accounts without visiting branches / offices of MMFL or meeting its officials.

vi. "Obtaining certified copy of Officially Valid Document (OVD)" – Means comparing the copy of OVD with the original and recording the same on the copy by authorized officer of MMFL.

vii. "Offline verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as per clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

viii. "Senior Management"

a. Senior Management for the purpose of the Policy shall constitute MD & CEO, CS, CFO, CTO, COO, Head – Operations, Head- Compliance and Head- Risk Management.

ix. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.

5. KEY ELEMENTS OF THE POLICY

As mentioned in the scope above, this Policy is applicable to all business operations and services including DP services, Money Transfer Services, etc and also applicable to business verticals of MMFL and it is to be read in conjunction with related operational guidelines issued from time to time.

Four Key elements

1. Customer Acceptance Policy;
2. Customer Identification Procedures;
3. Monitoring of Transactions; and
4. Risk management

Customer Acceptance Policy (CAP)

1. No account is opened in anonymous or fictitious/ benami name(s);
2. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk customers requiring very high level of monitoring, e.g. Politically Exposed Persons may, if considered necessary, be categorized even higher;
3. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
    i. Not to open an account or close an existing account where we are unable to apply appropriate customer due diligence measures
    ii. Circumstances in which a customer is permitted to act on behalf of another person/entity, as in the case of power of attorney holders, should be clearly spelt out in conformity with the established law and practice of banking.
    iii. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

The above can be met if we maintain a profile for each new customer based on risk categorization that could be a part of initial documentation.

Risk Level Categorization

The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk.

The profile of new customers will be prepared on risk categorization basis.

Such profile will contain the following information about the new customers:

• Customer’s Identity

• Social/Legal and financial status of the customer

• Nature of the business activity

• Information about the business of the customer’s clients and their locations

While preparing customer profile the Company shall seek only such information from the customer which is relevant to the risk category and is not intrusive to the customer.

The nature and extent of due diligence will depend on the risk perceived. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile as in the case of salaried employees , may be categorized as low risk.

Customers who are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, sources of funds and his client profile etc. We need to apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive ‘due diligence’ for higher risk customers, especially those for whom the sources of funds are not clear.

In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) and jewelers should also be categorized ‘high risk’ requiring enhanced due diligence. We are also required to subject these ‘high risk accounts’ to intensified transaction monitoring. High risk associated with such accounts should be taken into account by branches to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-ND.

Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. We need to obtain sufficient information necessary to establish, to our satisfaction, the identity of each new

customer, whether regular or occasional, and the purpose of the intended nature of relationship.

For individuals, we should obtain sufficient identification data to verify the identity of the customer, through any of the following physical documents

a. Passport

b. Voter's Identity Card

c. Driving license.

d. Aadhar Card (for address proof)

For individuals, we should obtain sufficient data to verify the address of the customer, through any of the following:

I. NPR (National Population Registration) Card
II. Ration Card with or without photo
III. Pension payment orders
IV. Credit Card Statement- not more than 3 months old
V. Salary slips with address (latest)
VI. Electricity Bill (latest)
VII. Landline Telephone Bill/Mobile bill - not more than 3 months old
VIII. Bank Pass Book/Account statement (latest)
IX. Rent Agreement (latest)
X. Gas Bill (latest).
XI. Photo identity Cards issued to bonafide students by a University, approved by the University Grants Commission (UGC) and/or an Institute approved by All India Council for Technical Education (AICTE).
XII. Government/Defence ID Card

For customers that are legal persons or entities wherever applicable, we should

(i) verify the legal status of the entity through proper and relevant documents;

(ii) verify that any person purporting to act on behalf of the entity is so authorized and identify and verify the identity of that person;

(iii) Understand the ownership and control structure of the customer and determine who are the natural persons -who ultimately control the legal person.

(iv) Collect the PAN details and also verify details of the customer for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees Five Lakhs, whether conducted as a single transaction or several transactions that appear to be connected.

(v) Periodic KYC updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers

Monitoring of Transactions

1. Ongoing monitoring is an essential element of effective KYC procedures. However, the extent of monitoring will depend on the risk sensitivity of the account

2. Branches must maintain proper record of all cash transactions (deposits and withdrawals) of Rs.10 lakh and above.

The internal monitoring system should have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a regular basis.

Risk Management

1. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

2. The internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

3. The audit machinery will be staffed adequately with individuals who are well-versed in such policies and procedures.

4. Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The

compliance in this regard may be put up before the Audit Committee of the Board on quarterly intervals.

We have an ongoing employee training program to ensure that members of the staff are adequately trained in KYC procedures.

Customer Education

Implementation of KYC procedures requires to demand certain information from customers which may be of personal nature or which has hitherto never been called for. There is a need to educate the customer of the objectives of the KYC programme. The branch staff needs to be specially trained to handle such situations while dealing with customers.

MMFL shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, cognizance of the overall sector-specific vulnerabilities if any, that the regulator/supervisor may share from time to time shall be taken. The risk assessment exercise shall be conducted on a quarterly basis and parameters of the assessment shall be modified, in alignment with the outcome of the risk assessment exercise. MMFL shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall monitor the implementation of the controls and enhance them, if necessary.

7. CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS

All the information collected from the Customers by MMFL shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the Customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that behalf. Information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer. Exception to the confidentiality of customer information shall be as under:

a. Where disclosure is under compulsion of law.

b. Where there is a duty to the public to disclose.

c. The interest of the company requires disclosure.

d. Where the disclosure is made with express or implied consent of the customer.

8. MAINTENANCE OF RECORDS OF TRANSACTIONS

MMFL take all reasonable steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules thereunder. MMFL shall

a. maintain all necessary records of transactions between MMFL and the customer, both domestic and international, for at least five years from the date of transaction or any other higher periods specified in any other law

b. preserve the records pertaining to the identification of the Customers and their addresses obtained while opening the account and during business relationship, for at least five years after the business relationship is ended.

c. Make available the identification records and transaction data to the competent authorities upon request;

d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005)

e. maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit reconstruction of individual transaction, including the following: (i) the nature of the transactions. (ii) the amount of the transaction and the currency in which it was denominated. (iii) the date on which the transaction was conducted; and (iv) the parties to the transaction.

f. MMFL have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities. g. Maintain records of the identity and address of its Customers, and records in respect of transactions referred to in Rule 3 of PML Rules, in hard or soft format.

9. GENERAL

Appointment of Designated Director &Principal Officer

We have appointed the Managing Director as the Designated Director to ensure overall compliance with the obligations imposed under PML Act and the Rules and the Person in charge of the Vigilance Department as Principal Officer who shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

Reporting to Financial Intelligence Unit - India

The Principal Officer will report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats

Where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of PMLA rules, such officer shall furnish information in respect of such transactions to the Director, FIU-IND, within the prescribed time.

A copy of all information furnished shall be retained by the Principal Officer for the purposes of official record.

10. STAFF and MANAGEMENT RESPONSIBILITIES – OFFENCE OF MONEY LAUNDERING

Staff and management shall take note that whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of offence of Money Laundering shall be subjected to appropriate internal disciplinary proceedings which may lead up to termination of service over and above the penalties under the relevant statutory Acts/Rules/ Regulations which includes punishment of being criminally proceeded against with and punishable with rigorous imprisonment and also liable to fine.

11. CDD PROCEDURE AND SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

MMFL shall capture the KYC information for uploading the data pertaining to all new individual accounts opened on or after 1/4/2017 with the CKYCR in the manner mentioned in the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time. Additionally, MMFL shall also upload KYC records pertaining to accounts of Legal Entities opened on or after April 1, 2021, with CKYCR in such manner as specified under the PML Rules.

MMFL shall also ensure that during periodic updation of the Customers, the Customers are migrated to the current CDD standard as applicable to MMFL. Government of India has authorized the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.

12. TRAINING PROGRAMME

MMFL shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and should have an ongoing employee training programs so that members of the staff are adequately trained in KYC/AML/CFT procedures. Training requirements shall have different focuses for front line staff, Compliance Staff and officer/staff dealing with new Customers so that all concerned fully understand the rationale behind the KYC policies and implement them consistently. Such training may be a mix of in-house as well as through external agencies, as the case may be.

13. COMPLIANCE WITH POLICY NORMS

a. MMFL's internal audit and compliance functions shall periodically evaluate the level of adherence to the KYC policies and procedures. The compliance function and audit function together shall provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements. The Audit Committee of the Board shall review adherence to the KYC guidelines at quarterly intervals.

b. Internal Audit shall on a yearly basis conduct an evaluation of compliance functions of policies and procedures including legal and regulatory requirements.

****