**MUTHOOTTU MINI FINANCIERS LTD**

# 'Know Your Customer' Policy

**Reviewed in the Meeting of Board of Directors held on 13-11-2020**

## The objective

The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards necessitating a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board. The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

## Scope and Application of the Policy

The scope of this policy is:

• To lay down explicit criteria for acceptance of customers.

• To establish procedures to identify of individuals/non-individuals for opening of account.

• To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.

• To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

## 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 categorised 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 categorisation, 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 categorised 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, his address/location through the following:

a. Ration card
b. Passport
c. PAN card
d. Voter’s Identity Card
e. Driving license.
f. Telephone Bill ( for address proof)
g. Bank account statement (for address proof)
h. Aadhar Card (for address proof)

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. We may prescribe threshold limits for a particular category of accounts, as in the case of repledger and pay particular attention to the transactions which exceed these limits.
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 fortnightly 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 programme 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 front desk staff needs to be specially trained to handle such situations while dealing with customers.

**KYC for the Existing Accounts**

Where we are unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, we will be forced to consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

With a view to preventing branches being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing, whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, Branches should carry out full scale customer due diligence (CDD) before opening an account. In case of need, branches could approach their RMs and CO for further guidance.

Branches should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. It is clarified that in the circumstances when a branch believes that it would no longer be satisfied that it knows the true identity of the account holder, the respective branch should notify CO for necessary reporting.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP (Politically Exposed Person), branches should obtain CO approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

The instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

**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 Audit 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.

**********