Mpee Finance Private Limited

Know Your Customer (KYC) Guidelines &
Anti-Money Laundering Standards (AML) Policy

Table of Contents

Contents

CHAPTER – I

1. Preamble

The Reserve Bank of India (RBI) had advised all the NBFCs to ensure that a proper policy framework on Know Your Customer and Anti Money Laundering measures is formulated and put in place with approval of the Board. The policy was to lay down the systems and procedures to help control financial frauds, identify money laundering and suspicious transactions, combating financing of terrorism and careful scrutiny / monitoring of large value of cash transactions.

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, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company on April 10, 2024. This will also comply with the modifications effected by RBI to its KYC Master Directions RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No. 81/14.01.001/2015-16 dated 10th May 2021.

This policy is applicable to all categories of products and services offered by the Company.

2. Scope and application of the policy

The scope of this policy is:

2.1. To lay down explicit criteria for acceptance of customers.

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

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

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

To fulfil the scope, the following elements will be incorporated into our policy:

- Customer Acceptance Policy,
- Risk Management,
- Customer Identification Procedures (CIP),
- Customer Due Diligence (CDD) Procedure,
- Record Management,
- Reporting Requirements to Financial Intelligence Unit – India, and
- Other Instructions.

3. Compliance with the policy

3.1 The Company shall ensure that the compliance with this Policy in all its products and processes.

3.2 The Company shall ensure that the decision-making functions are not outsourced.

3.3 Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.

3.4 Submission of quarterly compliance status to the Compliance Officer.

3.5 All the procedures namely, Customer Due Diligence (CDD) procedure, risk management, customer identification process shall be carried out for all the business verticals including co-lending.

4. Definitions

4.1 "**Aadhaar number**" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

4.2 "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

4.3 "**Authentication**", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

4.4 **Beneficial Owner** (BO):

4.4.1. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons,

has/have a controlling ownership interest or who exercise control through other means.

Explanation- for the purpose of this sub-clause-

a) "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

b) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

4.4.2. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

4.4.3. Where the **customer is an unincorporated association** or **body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

4.4.4. Where the **customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

4.5 "**Certified Copy**" - Obtaining a certified copy by the MAFSIPL shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the MAFSIPL as per the provisions contained in the Act.

Provided that in case of **Non-Resident Indians** (NRIs) and **Persons of Indian Origin** (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
b) branches of overseas banks with whom Indian banks have relationships,
c) Notary Public abroad,
d) Court Magistrate,
e) Judge,
f) Indian Embassy/Consulate General in the country where the non-resident customer resides.

4.6 "**Central KYC Records Registry**" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

4.7 "**Designated Director**" means a person designated by the MAFSIPL to ensure overall compliance with the obligations imposed under chapter IV of the PML Act.

4.8 "**Digital KYC**" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the MAFSIPL as per the provisions contained in the Act.

4.9 "**Digital Signature**" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

4.10 "**Equivalent e-document**" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

4.12 "**Non-profit organisations**" (NPO) means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

4.13 "**Officially Valid Document**" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

4.13.1. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

4.13.2. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; and

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

4.13.3. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at '4.13.2' above.

4.13.4. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

4.14 "**Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

4.15 "**Person**" has the same meaning assigned in the Act and includes:

4.15.1. an individual,

4.15.2. a Hindu undivided family,

4.15.3. a company,

4.15.4. a firm,

4.15.5. an association of persons or a body of individuals, whether incorporated or not,

4.15.6. every artificial juridical person, not falling within any one of the above persons (4.15.1 to 4.15.5), and

4.15.7. any agency, office or branch owned or controlled by any of the above persons (4.15.1 to 4.15.6).

4.16 "**Principal Officer**" means an officer nominated by the MAFSIPL, responsible for furnishing information as per rule 8 of the Rules.

4.17 "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

4.17.1. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

4.17.2. appears to be made in circumstances of unusual or unjustified complexity; or

4.17.3. appears to not have economic rationale or bona-fide purpose; or

4.17.4. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

4.18 "**Transaction**" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

4.18.1. opening of an account;

4.18.2. entering into any fiduciary relationship;

4.18.3. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

4.18.4. establishing or creating a legal person or legal arrangement.

4.19 "**Video based Customer Identification Process** (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the MAFSIPL by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this policy.

4.20 "**Customer**" means a person who is engaged in a financial transaction or activity with a MAFSIPL and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

4.21 "**FATCA**" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

4.22 "**KYC Templates**" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

5. Money Laundering and Terrorist Financing Risk Assessment

5.1. MAFSIPL 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 for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should 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, MAFSIPL shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with MAFSIPL from time to time.

5.2. The risk assessment by the MAFSIPL shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the MAFSIPL. The risk categorisation based on various customer profiles has been defined later in Chapter III of this document.

5.3. The summary of the risk assessment exercise shall be put up to the Board or Audit Committee of the Board to which power in this regard has been delegated on an annual basis and should also be available to competent authorities and self-regulating bodies.

5.4. MAFSIPL shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, MAFSIPL shall monitor the implementation of the controls and enhance them if necessary.

CHAPTER – II

6. Customer Acceptance Policy

Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, MAFSIPL shall ensure that:

6.1 No account is opened in anonymous or fictitious/benami name.

6.2 No account is opened where the MAFSIPL is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer.

6.3 No transaction or account-based relationship is undertaken without following the CDD procedure.

6.4 The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

6.5 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

6.6 MAFSIPL shall apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a MAFSIPL desires to open another account with the same MAFSIPL, there shall be no need for a fresh CDD exercise.

6.7 CDD Procedure is followed for all the joint account holders, while opening a joint account.

6.8 Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

6.9 Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

6.10 Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

6.11 Where an equivalent e-document is obtained from the customer, MAFSIPL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

CHAPTER – III

7. Risk Management

7. For Risk Management, MAFSIPL shall have a risk-based approach which includes the following:

7.1 Customers shall be categorised as low, medium, and high-risk category, based on the assessment and risk perception of the MAFSIPL.

7.2 Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's 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.

7.3 The risk-based categorization of a customer based on the KYC documents is mentioned below, subject to any regulatory requirement as may be specified from time to time:*

Low Risk	Low Risk individual customers are those individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and the transactions with them by and large conform to known profile. These include following: 1. Salaried Employee 2. Self Employed Individuals/Prop Firms 3. Government Department & Government Owned Companies 4. Limited Companies (Public & Private) 5. Partnership Firm (Registered Deed). 6. Loans to NRIs up to Rs. 25 Lakhs, in which repayment is through the NRO Account & no limit if repayment is from overseas remittance.
Medium Risk	1. NGOs, trusts, charities and organizations receiving donations 2. Trust/Societies 3. High net worth individuals (investible surplus more than Rs. 1.00 Crore) 4. Companies having close family shareholding or beneficial ownership. 5. Loans to NRIs above Rs. 25 Lakhs, where repayment of loan is through NRO Account.
High Risk	1. Politically Exposed Persons (PEP), 2. Family members and close relatives of PEP,

	3. Very high cash transactions (Rs. 10 Lakhs) and suspicious transactions reported to FIU-IND, 4. Persons with dubious reputation as per public information available, 5. Persons whose sources of income are not clear, 6. Non-face to face meeting customers.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same may be specified in the Credit Policy.

The Recommendations made by the Financial Action Task Force (FATF) on Anti-money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards should also be used in risk assessment.

Chapter – IV

8. Customer Identification Procedure (CIP)

8. MAFSIPL shall undertake identification of customers in the following cases:

8.1 Commencement of an account-based relationship with the customer.

8.2 When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

8.3 MAFSIPL shall ensure that introduction is not to be sought while opening accounts.

8.4 Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

8.5 Adequate steps are taken by MAFSIPL to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

8.6 The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

Chapter – V

Customer Due Diligence (CDD) Procedure

Part I

9. Customer Due Diligence (CDD) Procedure in case of Individuals

9. MAFSIPL shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

9.1 the Aadhaar number where,

9.1.1 he/she is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

9.1.2 he/she decides to submit his Aadhaar number voluntarily to MAFSIPL notified under first proviso to sub-section (1) of section 11A of the PML Act.

9.2 the proof of possession of Aadhaar number where offline verification can be carried out; or

9.3 the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

9.4 the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

9.5 such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the MAFSIPL:

Provided that where the customer has submitted,

i) Aadhaar number under clause (9.1) above to MAFSIPL notified under first proviso to sub-section (1) of section 11A of the PML Act, MAFSIPL shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he/she may give a self-declaration to that effect to the MAFSIPL.

ii) An equivalent e-document of any OVD, MAFSIPL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annex I**.

iii) Any OVD or proof of possession of Aadhaar number under clause (9.3) above where offline verification cannot be carried out, the MAFSIPL shall carry out verification through digital KYC as specified under **Annex I**.

10. Accounts opened using OTP based e-KYC

10.1 There must be a specific consent from the customer for authentication through OTP.

10.2 If the CDD procedure as mentioned above is not completed within a year, in respect of loan accounts, the same shall be closed immediately.

10.3 Further, while uploading KYC information to CKYCR, MAFSIPL shall clearly indicate that such accounts are opened using OTP based e-KYC.

10.4 MAFSIPL shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

Part II

11. Customer Due Diligence (CDD) Procedure in case of Sole Proprietary firms

11.1 For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

11.2 In addition to the (12.1) above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

11.2.1 Registration certificate

11.2.2 Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

11.2.3 GST certificate,

11.2.4 GST and income tax returns.

11.2.5 IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

11.2.6 Utility bills such as electricity, water, landline telephone bills, etc.

Part III

12. Customer Due Diligence (CDD) Procedure in case of Legal Entities

12.1 For opening an account of a **company**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

12.1.1 Certificate of incorporation

12.1.2 Memorandum and Articles of Association

12.1.3 Permanent Account Number of the company

12.1.4 A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

12.1.5 Documents, as specified in **Clause 9**, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

12.2 For opening an account of a **partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

12.2.1 Registration certificate

12.2.2 Partnership deed

12.2.3 Permanent Account Number of the partnership firm and

12.2.4 Documents, as specified in **Clause 9**, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

12.3 For opening an account of a **trust**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

12.3.1 Registration certificate

12.3.2 Trust deed

12.3.3 Permanent Account Number or Form No.60 of the trust

12.3.4 Documents, as specified in **Clause 9**, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

12.4 For opening an account of an **unincorporated association** or a **body of individuals**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

12.4.1 Resolution of the managing body of such association or body of individuals

12.4.2 Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals

12.4.3 Power of attorney granted to transact on its behalf

12.4.4 Documents, as specified in **Clause 9**, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and

12.4.5 Such information as may be required by MAFSIPL to collectively establish the legal existence of such an association or body of individuals.

13. Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to verify his/her identity shall be undertaken keeping in view the following:

13.1 Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

13.2 In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

14. Periodic Updation

MAFSIPL shall adopt a risk-based approach for periodic updation of KYC. However, periodic 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 from the date of opening of the account / last KYC updation.

14.1 In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the MAFSIPL or customer's mobile number registered with the MAFSIPL.

14.2 In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the MAFSIPL, and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, Aadhar validation etc.

14.3 Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the MAFSIPL and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

14.4 **Accounts of Politically Exposed Persons** (PEP): Special care and diligence will be taken in respect of Politically Exposed Persons. Generally, the MAFSIPL would not open accounts of PEP. Decision to deal with such persons as a Customer shall be taken up at a senior management level and shall be subjected to enhanced monitoring.

14.5 **Customer Education**: MAFSIPL should prepare specific literature / pamphlets etc., to educate the customer of the objectives of the KYC program. The frontline lending and operating managers should be fully equipped with the compliance requirements of KYC guidelines in respect of new customer acquisition and shall adhere to the Customer Identification & Acceptance procedure.

Chapter – VI

15. Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. MAFSIPL shall,

15.1 maintain all necessary records of transactions between the MAFSIPL and the customer, both domestic and international, for at least eight years from the date of transaction,

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

15.3 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),

15.4 evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities,

15.5 maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Chapter – VII

16. Reporting Requirements to Financial Intelligence Unit – India

MAFSIPL shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website http://fiuindia.gov.in.

MAFSIPL shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and also 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 and officer/staff dealing with new customers so that all concerned fully understand the rationale behind the KYC policies and implement them consistently.

16.1 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 as designed and circulated by RBI at the following address:

To,
Director, FIU-IND,
Financial Intelligence Unit, India, 6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi - 110021

Chapter – VIII

17. Procedure to undertake Video based Customer Identification Process (V-CIP)

17.1 Customer Due Diligence (CDD) in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

17.2 MAFSIPL opting to undertake V-CIP, shall adhere to the following minimum standards:

17.2.1 **V-CIP Infrastructure**

a. MAFSIPL should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the MAFSIPL and the V-CIP connection and interaction

shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

b. MAFSIPL shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

c. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

d. The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

e. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the MAFSIPL. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

f. The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

17.2.2 **V-CIP Procedure**

a) MAFSIPL shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the MAFSIPL specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

b) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

c) The authorised official of the MAFSIPL performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

   i) OTP based Aadhaar e-KYC authentication,

   ii) Offline Verification of Aadhaar for identification,

   iii) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer, and

   iv) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

d) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

e) MAFSIPL shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

f) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

g) The authorised official of the MAFSIPL shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

17.2.3 **V-CIP Records and Data Management**

The entire data and recordings of V-CIP shall be stored in a system / system located in India. MAFSIPL shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

18. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

18.1 In terms of provision of Rule 9(1A) of PML Rules, MAFSIPL shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

18.2 Once KYC Identifier is generated by CKYCR, MAFSIPL shall ensure that the same is communicated to the individual/Legal Entity as the case may be.

18.3 Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to a MAFSIPL, with an explicit consent to download records from CKYCR, then such MAFSIPL shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

18.3.1 there is a change in the information of the customer as existing in the records of CKYCR;

18.3.2 the current address of the customer is required to be verified;

18.3.3 MAFSIPL considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

19. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, MAFSIPL shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

19.1 Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution,

19.2 Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

19.3 Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

19.4 Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. MAFSIPL may take note of the following:

19.4.1 updated Guidance Note on FATCA and CRS

19.4.2 a press release on 'Closure of Financial Accounts' under Rule 114H (8).

20. Customer due diligence by third party

In compliance of the KYC regulations, MAFSIPL may rely on the customer due diligence done by third parties, which are regulated entities, for verifying identity of customers at the time of commencement of account-based relationship, subject to the following conditions.

20.1 Records or information of the customer due diligence carried out by the third party is obtained within 2 days from the third party or from Central KYC Records Registry.

20.2 MAFSIPL is satisfied that copies of the identification data and other relevant documents relating to the customer due diligence requirements will be available from the third party up on request without delay.

20.3 The third party is regulated, supervised or monitored and has capabilities to comply with the customer due diligence and record keeping requirements as prescribed in the Prevention of Money Laundering Act.

20.4 The third party shall not be based in a country or jurisdiction assessed as high risk.

****

ANNEX I: Digital KYC Process

A. MAFSIPL shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the MAFSIPL.

B. The access of the Application shall be controlled by the MAFSIPL and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by MAFSIPL to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the MAFSIPL or vice-versa. The original OVD shall be in possession of the customer.

D. MAFSIPL must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the MAFSIPL shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by MAFSIPL) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the MAFSIPL shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from

UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the MAFSIPL shall not be used for customer signature. The MAFSIPL must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the MAFSIPL. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the MAFSIPL, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the MAFSIPL shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the MAFSIPL who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

ANNEX – II: List of suspicious transactions

Broad categories of reasons for suspicion and examples of suspicious transactions generally observed in Non- Banking Financial Companies are indicated as under:

1. Identity of client
    - 1.1 False identification documents,
    - 1.2 Identification documents which could not be verified within reasonable time, and
    - 1.3 Accounts opened with names very close to other established business entities.
2. Background of Client: Suspicious background or links with known criminals.
3. Activity in accounts
    - 3.1 Unusual activity compared with past transactions- Sudden activity in dormant accounts, and
    - 3.2 Activity inconsistent with what would be expected from declared business.
4. Nature of transactions
    - 4.1 Unusual or unjustified complexity,
    - 4.2 No economic rationale or bonafide purpose,
    - 4.3 Frequent cash transactions, and
    - 4.4 Nature of transactions inconsistent with what would be expected from declared business.
5. Value of Transactions
    - 5.1 Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
    - 5.2 Value inconsistent with the client's apparent financial standing.
6. Indicators of Suspicious Transactions
    - 6.1 Reluctant to part with information, data and documents,
    - 6.2 Submission of false documents, purpose of loan and detail of accounts,
    - 6.3 Reluctance to furnish details of source of funds,
    - 6.4 Payment of initial contribution through unrelated third-party account,
    - 6.5 Suggesting dubious means for sanction of loan,
    - 6.6 Where transactions do not make economic sense, and
    - 6.7 Frequent request for change of address.