MIRAE ASSET
Financial Services

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

**Version 5.0**

May 2026

| Document Control | |
|---|---|
| **Document** | KYC and AML Policy |
| **DOC ID/ Number** | MAFS/Risk & Compliance/May 2026/ Version 5.0 |
| **Policy Adherence by** | All |
| **Effective date** | July 12, 2021 |
| **Last Review date** | May 06, 2026 |
| **Approved by** | Board of Directors |

## 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.

This policy has been framed for attaining the following broad objectives:

- To prevent criminal elements from using Company for money laundering activities.
- To enable the Company to know and understand its customers and financial dealings in a better manner, which in turn, shall help manage the risks prudently.
- To establish appropriate, effective and efficient controls for detection and reporting of suspicious activities in accordance with the applicable laws / laid down procedures.
- To comply with the applicable regulations and operate within the regulatory framework prescribed by the regulator.
- To ensure importance of KYC / AML / Combating the Financing of Terrorism ["CFT"] is established with the concerned employees / persons dealing with customers on behalf of the Company.
- To ensure adequate training to the employees / persons dealing with customers on behalf of the Company in the KYC / AML / CFT procedures.
- To update and ensure continuing adherence to the Directions as issued by RBI from time to time after deliberations by the board.

This Policy supersedes and replaces all earlier internal KYC / AML policies framed pursuant to the erstwhile Master Direction – Know Your Customer (KYC), 2016, which stands repealed. This Policy is aligned with and issued pursuant to the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, as amended from time to time.

## 2. 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 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.

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,
- Monitoring of Transactions
- Record Management,
- Reporting Requirements to Financial Intelligence Unit – India, and
- Other Instructions.

This policy shall be applicable organization-wide to all employees / persons dealing with customers on behalf of the Company.

This policy is to be read in conjunction with the operational guidelines issued by RBI and FIU-IND from time to time. The content of this policy shall always be read in tandem / auto-

corrected with the changes / modifications as may be advised by RBI and / or by PMLA and amendments of the Directions, from time to time.

## 3. Compliance with the Regulations

- The Company ensures compliance with this Policy to comply with the regulations in all its products and processes.
- The Company ensures decision-making functions are not outsourced.
- Specifies as to who constitutes 'Senior Management' for the purpose of KYC compliance.
- Submission of quarterly compliance status to the Compliance Officer.
- 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.
- Allocates responsibility for effective implementation of policies and procedures.
- System for independent evaluation of the compliance function and policies and procedures, including legal and regulatory requirements.
- Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
- Submission of quarterly audit notes and compliance to the Audit Committee.

## 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 10 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 10 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 10 per cent 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 MAFS 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 MAFS 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.

Where KYC records are downloaded from the Central KYC Records Registry (CKYCR), the Company shall rely on the identity and/or address verification carried out by the Regulated Entity that last uploaded or updated such records in CKYCR. Notwithstanding such reliance,

the Company shall remain fully responsible for all other aspects of Customer Due Diligence (CDD), ongoing monitoring, risk assessment, and compliance with the Prevention of Money-laundering Act, 2002 and the RBI KYC Directions.

4.7 "Designated Director" means a person designated by the MAFS 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 MAFS 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 license, 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 MAFS, 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 MAFS 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 MAFS 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.

*Note: Terms used under this policy and not defined hereunder shall have the same meaning as assigned to them under the KYC Directions, PMLA Act 2002 or Rules thereunder, Aadhar Act, 2016 or rules made thereunder and any other applicable provisions.*

## 5. Designations, responsibilities and management

The Board of Directors of the Company shall be responsible for the purposes of compliance with and overview of the systems placed for such compliance with the KYC / AML / CFT procedures of the Company.

The Principal Officer ["PO"] of the Company, so appointed, shall be responsible for effective and complete implementation of the procedures prescribed under this policy. The PO shall make his reporting to the Senior Management i.e. the board of directors including "Designated Director".

The Company shall devise the internal audit function/Specialized Internal control systems in a manner, which shall extensively include verification of KYC / AML / CFT procedures undertaken by the Company, and its compliance with this policy and regulatory requirements.

## 6. APPOINTMENTS

### DESIGNATED DIRECTOR

The Company has appointed Whole Time Director of the Company, as the Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules, as nominated by the Board of Directors.

The Designated Director of the Company shall not be the same as the Principal Officer of the Company at any point as guided in the Directions.

The Designated along with other members of "Senior management" shall perform an overview function of the compliance with policies and shall evaluate the Quarterly Audit Notes and compliance to the Audit Committee prepared by the Principal Officer and other authorities to whom internal audit function is assigned.

**PRINCIPAL OFFICER**

The Company shall designate a senior employee as a Principal Officer (PO), who shall be located at Corporate Office and not be the same as the Designated Director, for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. PO shall maintain close liaison with enforcement agencies, NBFCs, Credit Information Companies, FIU-Ind, and any other institutions involved in the fight against money laundering and CFT.

**CHANGE IN OFFICERS**

The Company shall intimate the Regional Office of RBI, alongwith the office of Financial Intelligence Unit – India ["FIU-Ind"], of any change in the Principal Officer and / or Designated Director of the Company and / or their details within one month of the date of such change**.**

**7. UNIQUE CUSTOMER IDENTIFICATION CODE ["UCIC"]/ Customer Identification Number ["CIF"/ "Cust ID"]**

The Company shall assign a Unique Customer Identification Code ["UCIC"] / Customer Identification Number ["CIF"/ "Cust ID"] to both existing as well as new customers, in order to link all account-based relationships / transactions to the customer.

## 8. Money Laundering and Terrorist Financing Risk Assessment

MAFS 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 Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment shall explicitly include assessment of Proliferation Financing (PF) risks and shall be reviewed upon occurrence of material triggers including launch of new products, adoption of new technologies, entry into new geographies, regulatory advisories, or occurrence of significant fraud or compliance-related events.

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

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

The summary of the risk assessment exercise shall be put up to the Board on an annual basis and should also be available to competent authorities and self-regulating bodies.

MAFS 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, MAFS shall monitor the implementation of the controls and enhance them if necessary.

# CHAPTER – II

## 9. Customer Acceptance Policy

Without prejudice to the generality of the aspect that Customer Acceptance Policy (CAP) may contain, MAFS shall ensure that:

- No account is opened in anonymous or fictitious/benami name.
- No account is opened where the MAFS 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.
- No transaction or account-based relationship is undertaken without following the CDD procedure.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- 'Optional'/additional information, where such information requirement has not been specified in the policy is obtained with the explicit consent of the customer after the account is opened.
- MAFS shall apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a MAFS desires to open another account with the same MAFS, there shall be no need for a fresh CDD exercise.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- 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.

- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, MAFS shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

Implementation of CAP should not be too restrictive and result in denial of the Company services to general public. The decision to open an account / enter into a transaction with Politically Exposed Persons ["PEP"] shall be taken by any one of the Directors on the Board of the Company.

It may however, be necessary to have suitable built in safeguards to avoid any harassment to customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

Where a suspicion of money laundering or terrorist financing, and Principal Officer/Officer/Employee of the company reasonably believes that performing the CDD process will tip-off the customer, they shall escalate the matter and not pursue the CDD process. Appropriate authority shall proceed to file an STR with the FIU India.

## CHAPTER – III

## 10. Risk Management

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

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

- Broad principles have been laid down for effective risk-categorisation of customers, which are

  1. The categorization shall be made without prejudice to the Fair Practice Code of the company.

  2. The categorization matrix shall be practical and updated.

  3. The parameters for customer categorization shall be evaluated on periodic basis and prevailing industry circumstances

  4. Risk Categorization shall be made/updated post obtaining all the documents/information from the customer as well as internal research.

  5. Risk Category may be upgraded/downgraded at any time considering the facts available and with appropriate reporting to the Risk Management Committee.

  6. The risk categorization system shall consider other principles guiding the operations of the company

- 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.

- The risk categorisation and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

- 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. This shall be the driving principle to classify the customers in this category.

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.

7. Any Person not identified as Low Risk/ Medium Risk Customer, till review of documents produced indicate classification as a Low Risk/Medium Risk category classification.

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

## 11. Customer Identification Procedure (CIP)

Customer Identification means identifying the Customer/Beneficial Owner and verifying his/her/its identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship at the time of Commencement of an account-based relationship.

Apart from CIP conducted at the commencement of account-based relationship, the company may conduct a CIP at any point of time when it has reasons to believe or suspects any of following:

MAFS shall undertake identification of customers in the following cases:

- Commencement of an account-based relationship with the customer.
- When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

- MAFS shall ensure that introduction is not to be sought while opening accounts.
- 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.
- Adequate steps are taken by MAFS 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.
- 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.

**Special CIP Requirements**

**Accounts of Politically Exposed Persons (PEPs) resident outside India**

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

The Company shall gather sufficient information on any Person/Customer of this category intending to establish a relationship and check all the information available on the Person in the public domain. The Company shall verify the identity of the Person and seek information about the sources of funds before accepting the PEP as a Customer. The decision to provide financial services to an account for PEP shall be taken at the Board of Directors level and shall be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

**Accounts of non-face-to-face Customers**

In the case of non-face-to-face Customers, apart from applying the usual Customer Identification Procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for

In the case of cross-border Customers, there is the additional difficulty of matching the Customer with the documentation and the Company may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

**Trust/Nominee or Fiduciary Accounts**

The Company shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the Persons on whose behalf they are reacting, as also obtain details of the nature of the trust or other arrangements in place. The Company shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any Person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a foundation, branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the Customer Identification Procedures.

**Accounts of companies and firms**

The Company needs to be vigilant against business entities being used by individuals as a front for maintaining accounts with the Company. The Company mandatorily has to examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it shall not be necessary to identify all the shareholders.

# Chapter – V

# Customer Due Diligence (CDD) Procedure

## Part I

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

MAFS 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:

Voluntary Nature of Aadhaar

The Company shall not deny services solely on the ground that a customer does not possess or does not wish to submit Aadhaar. Submission of Aadhaar shall be mandatory only in cases covered under Section 7 of the Aadhaar Act for receipt of notified subsidies or benefits.

- the Aadhaar number where,
    - 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
    - he/she decides to submit his Aadhaar number voluntarily to MAFS notified under first proviso to sub-section (1) of section 11A of the PML Act.
- the proof of possession of Aadhaar number where offline verification can be carried out; or

- 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; or
- the KYC Identifier with an explicit consent to download records from CKYCR; and,
- the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- 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 MAFS.

Provided that where the customer has submitted

i) Aadhaar number above to MAFS notified to avail benefit under first proviso to sub-section (1) of section 11A of the PML Act, MAFS 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 MAFS.

ii) An equivalent e-document of any OVD, MAFS shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and in compliance with the Digital KYC as stated under Annex I

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

iv) KYC Identifier under clause (ac) above, the RE shall retrieve the KYC records online from the CKYCR

**Accounts opened using OTP based e-KYC**

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

- If the CDD procedure as mentioned above is not completed within a year, in respect of loan accounts, the same shall be closed immediately.
- Further, while uploading KYC information to CKYCR, MAFS shall clearly indicate that such accounts are opened using OTP based e-KYC.
- As a risk-mitigating measure the transaction alerts, OTP, etc., shall be sent only to the mobile number of the customer registered with Aadhaar. In case any customer wants to change registered mobile number, then an OTP will be sent to the existing email address of the customer registered with MAFS, and once validated, an OTP will be sent to the new mobile number provided by the customer for updation. Based on this confirmation the number will be updated. Similarly, for updation of email address, an OTP will be first sent to the registered mobile number provided to MAFS, and once validated an OTP will be sent to the new email address. Based on this any updation will be allowed.
- MAFS 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

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

- For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.
- 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:
    - Registration certificate(including Udyam Registration Certificate (URC) issued by the Government)
    - Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
    - GST certificate,
    - GST and income tax returns.
    - 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.
    - Utility bills such as electricity, water, landline telephone bills, etc.

## Part III

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

- For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    - Certificate of incorporation
    - Memorandum and Articles of Association
    - Permanent Account Number of the company
    - A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

- 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
- The names of the relevant persons holding senior management position; and
- The registered office and principal place of its business, if different.

- 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:
  - Registration certificate
  - Partnership deed
  - Permanent Account Number of the partnership firm and
  - 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
  - The names of all the partners and
  - The address of the registered office, and principal place of its business, if it is different.

- For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
  - Registration certificate
  - Trust deed
  - Permanent Account Number or Form No.60 of the trust
  - The names of the beneficiaries, trustees, settlor and authors of the trust,
  - Documents, as specified in paragraph 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
  - The address of the registered office of the trust, and
  - The list of trustees and documents, as specified under Clause 9, for those discharging the role as trustee and authorized to transact on behalf of the trust.

- 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:
    - Resolution of the managing body of such association or body of individuals
    - Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
    - Power of attorney granted to transact on its behalf
    - 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
    - Such information as may be required by MAFS to collectively establish the legal existence of such an association or body of individuals.
- For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:
    - Document showing name of the person authorised to act on behalf of the entity
    - Documents, as specified in paragraph 16, of the person holding an attorney to transact on its behalf and
    - Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

**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:

- 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 or is an entity resident in

jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

- 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.

**On-going Due Diligence**

MAFS shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

(a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
(c) High account turnover inconsistent with the size of the balance maintained.
(d) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, MAFS has adopted trackwizz/Screenzaa software to provide a comprehensive one stop solution for detection and monitoring of AML issues, this software uses industry renowned technology and domain centric expertise providing an appropriate innovative technology to support effective monitoring.

The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

(b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

**Updation/ Periodic Updation**

MAFS 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.

a) Individuals:

i. No change in KYC information: 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 MAFS, customer's mobile number registered with MAFS, digital channels (such as website, mobile application of MAFS), letter, etc.

ii. Change in address: 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 MAFS, customer's mobile number registered with the RE, digital channels (such as wesbite, mobile application of MAFS), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

Further, MAFS, at its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 4.10, for the purpose of proof of address, declared by the customer at the time of periodic updation.

iii. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. MAFS shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals:

i. No change in KYC information: In case of no change in the KYC information of the legal entity customer, a self-declaration in this regard shall be obtained from the legal entity customer through its email id registered with MAFS, digital channels (such as website, mobile application of MAFS), letter from an official authorized by the legal entity in this regard, board resolution, etc. Further, MAFS shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. Change in KYC information: In case of change in KYC information, MAFS shall undertake the KYC process equivalent to that applicable for on-boarding a new legal entity customer.

c) Additional measures: In addition to the above, MAFS shall ensure that,

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the MAFS are not as per the current CDD standards. Further, in case the validity of the CDD documents available with MAFS has expired at the time of periodic updation of KYC, MAFS shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

ii. Customer's PAN details, if available with MAFS, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. 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 MAFS and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, MAFS may consider making available the facility of periodic updation of KYC at any branch.

v. MAFS shall adopt a risk-based approach with respect to periodic updation of KYC.

d) MAFS shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit details of such update as well as documentary evidence (if any). This shall be done within 30 days of the update to the documents for the purpose of updating the records at MAFS' end.

In case of existing customers, MAFS shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which MAFS shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the RE shall give the customer an accessible notice and a reasonable opportunity to be heard.

Further, MAFS shall include, in its internal policy, appropriate relaxation(s) for
continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60
owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with MAFS gives in writing to MAFS that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, MAFS shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by MAFS till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

## Enhanced Due Diligence Procedure

**Enhanced Due Diligence (EDD) for non-face-to-face customer on-boarding (other than customer onboarding with Aadhar OTP based e-KYC ):**

EDD measures shall be undertaken by MAFS for non-face-to-face customer onboarding (other than customer onboarding with Aadhar OTP based e-KYC) as stated below:

a) V-CIP shall be provided as the first option to the customer for remote onboarding as a successful V-CIP shall be treated on par with face-to-face CIP as per RBI guidance.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

c) Apart from obtaining the current address proof, MAFS shall verify the current address through positive confirmation (through means such as address verification letter, contact point verification, deliverables, etc.) before allowing operations in the account.

d) MAFS shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

**Procedure for updation of registered mobile number and email address provided at the time of account opening**

In case any customer wants to change registered mobile number, then an OTP will be sent to the existing email address of the customer registered with MAFS, and once validated, an OTP will be sent to the new mobile number provided by the customer for updation. Based on this confirmation the number will be updated. Similarly, for updation of email address, an OTP will be first sent to the registered mobile number provided to MAFS, and once validated an OTP will be sent to the new email address. Based on this any updation will be allowed.

**Accounts of Politically Exposed Persons (PEPs)**

A. MAFS shall have the option of establishing a relationship with PEPs provided that:

(a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

(b) the identity of the person shall have been verified before accepting the PEP as a customer;

(c) the decision to open an account for a PEP is taken at a senior level in accordance with the MAFS' Customer Acceptance Policy;

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

(f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner

*Note: For this purpose, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.*

**Client accounts opened by professional intermediaries:**

MAFS shall ensure while opening client accounts through professional intermediaries, that:

(a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

(b) MAFS shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

(c) MAFS shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the MAFS.

(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of MAFS, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of MAFS, MAFS shall look for the beneficial owners.

(e) MAFS shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

(f) The ultimate responsibility for knowing the customer lies with MAFS.

## 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. MAFS shall,

- maintain all necessary records of transactions between the MAFS and the customer, both domestic and international, for at least eight years from the date of transaction,
- 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,
- 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),
- 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,
- 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.

*Note: here, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.*

The Company shall maintain proper records of the transactions as required under Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:

- All cash transactions of the value of more than Rupees Ten Lakhs (Rs. 10,00, 000/-) or its equivalent in foreign currency, though by policy the Company neither accept cash deposits nor in foreign currency

- All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees Ten Lakh or its equivalent in foreign currency.

- All transactions involving receipts by non-profit organizations of Rupees ten lakhs or its equivalent in foreign currency

- All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions

- All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity as the case may be.

- All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in Annex II.

The company shall update and verify if any of the customers have a direct/indirect connection to the list as mandatory for Unlawful Activities (Prevention)(UAPA) Act 1967 from time to time. The same shall be reported to Principal Officer by the employees and subsequently higher Authority in the company and seek guidance from RBI for further actions to be pursued.

For customers who are non-profit organisations, MAFS shall ensure that the details are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, MAFS shall

register the details on the DARPAN Portal. MAFS shall also maintain such registration records for a period of five years after the business relationship or the account has been closed, whichever is later.

## Chapter – VII

## 16. Reporting Requirements to Financial Intelligence Unit – India

MAFS 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 Company shall register on the FINnet portal, alongwith undertaking registration of the Principal Officer.

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.

MAFS 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; to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and

internationally. 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.

Further, promotion of an environment which fosters open communication and high integrity amongst the staff has been highlighted during on-boarding new employees.

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, alongwith necessary online filings:

To,
Director,
Financial Intelligence Unit, India,
–6th Floor, Tower-2,
Jeevan Bharati Building,
Connaught Place,
New Delhi-110001, INDIA
Telephone : 91-11-23314429, 23314459

The Company shall maintain strict confidentiality of the fact of furnishing / reporting details of suspicious transactions.

## 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 MAFS opting to undertake V-CIP, shall adhere to the following minimum standards:

17.2.1 V-CIP Infrastructure

a. MAFS 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 MAFS 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. MAFS 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 MAFS. 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 by empaneled auditors of Indian Computer Emergency Response Team (CERT-In). 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.

g. In case the facility is obtained from an outsourced vendor, MAFS shall ensure compliance with the RBI prescribed infrastructure norms. Where cloud deployment model is used, the ownership of data in such model shall be rretained and all the data including video recording is transferred to exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

17.2.2 V-CIP Procedure

a) MAFS 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 MAFS 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 MAFS 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. Following points shall be observed while performing offline verification:

- Aadhaar number shall be blacked out/redacted
- If XML file/Aadhar Secure QR code is provided for verification, it shall be ensured that the file/QR code is not older than 3 working days
- Fresh verification process shall be initiated if due to reasons, V-CIP could not be completed within 3 days.

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) MAFS 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 MAFS 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 (including credential of officer performing the V-CIP) and recordings of V-CIP shall be stored in a system / system located in India. MAFS 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.

V-CIP including liveness checks and facial recognition processes, shall be conducted in a non-discriminatory manner. No specific physical gesture shall be insisted upon, and the process shall ensure that persons with disabilities are not excluded from customer onboarding or periodic updation of KYC.

## 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, MAFS shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be.

18.2 Once KYC Identifier is generated by CKYCR, MAFS 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 MAFS, with an explicit consent to download records from CKYCR, then such MAFS 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 MAFS 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.

Further, the customers records shall be migrated to the current CDD standards at the time of periodic updation.

## 18A. Reporting to CERSAI

The Company shall register itself on CERSAI, and shall share all relevant information required, relating to the mortgages created in the favor of the Company.

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

Under FATCA and CRS, MAFS 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.

Further, MAFS shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, MAFS shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

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. MAFS 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, MAFS 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 MAFS 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.

**21. Secrecy Obligations and Sharing of Information:**

(a) MAFS shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, MAFS shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law,

ii. Where there is a duty to the public to disclose,

iii. Where the interest of RE requires disclosure, and

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

**********

# ANNEX I: Digital KYC Process

A. MAFS 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 MAFS.

B. The access of the Application shall be controlled by the MAFS 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 MAFS to its authorized officials.

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

D. MAFS 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 MAFS shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by MAFS) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the MAFS 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 MAFS shall not be used for customer signature. The MAFS 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 MAFS. 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

MAFS, 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 MAFS 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 MAFS 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.