MANAPPURAM ASSET FINANCE LIMITED (MAAFIN)

KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY LAUNDERING POLICY

	Version Control	
Version Number	**Description**	**Date**
Version 1.0	Know Your Customer (KYC) And Prevention Of Money Laundering Policy	01-04-2017
Version 2.0	Know Your Customer (KYC) And Prevention Of Money Laundering Policy	03-12-2024
Version 3.0	Know Your Customer (KYC) And Prevention Of Money Laundering Policy	21-03-2026

Effective Date	**21-03-2026**
Next Review Date	**Yearly**
Policy Owner	**Operations Department**
Reviewed By	**Policy Review Committee.**
Approved By	**Board**

Contents	

1.Introduction

RBI vide its Master Direction RBI/DOR/2025-26/361:DOR.AML.REC.No.280/14.01.003/2025- dated November 28, 2025 titled "Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025" has issued a consolidated circular on KYC & AML by incorporating all the directions issued by the RBI, hitherto, in the subject. In accordance with the Master Directions by Reserve Bank of India, all Regulated Entities (REs) including Manappuram Asset Finance Limited (MAAFIN) are required to put in place appropriate Policy and procedures to comply with the relevant Know Your Customer (KYC) norms and Customer Due Diligence (CDD) processes at the time of onboarding the Customer and also during the continued relationship with such Customer which includes monitoring of transactions in terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as well as the relevant norms as put out by SEBI which has also issued guidelines on AML standards to be followed by market intermediaries viz Depository Participants, Asset Management Companies etc. Accordingly, the Company has in place the Policy, which is further detailed below.

2.Policy Statement

MAAFIN is primarily engaged in retail finance and by nature of its business operations, the potential risks of money laundering, terrorist financing that it faces is relatively low. MAAFIN recognizes the importance of the AML programs and commits itself to inculcating a vigilant culture in combating money laundering to the extent applicable to the firm. Accordingly, it puts in place a detailed KYC & AML Policy and procedures hereunder in line with RBI Directions and Prevention of the Money Laundering Act, 2002 / Rules as amended from time to time as well that of the norms put out by the other relevant regulations that is applicable to its business operations, for the time being in force. A group-wide policy against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programs shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping- off, is implemented for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003).

3.Objectives

The Policy seeks to achieve the following objectives.

- ➔ To provide a framework for how the company, in its process of conducting business with Customers, will deal with the threat of money laundering and terrorism financing.

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

To comply with applicable laws and regulatory guidelines.

4.Scope

a. This Policy applies to all employees of MAAFIN, and third-party agents engaged by it for origination, fulfilment, collection, outsourcing agencies, etc. The Policy seeks to maintain high standards of conduct within the Company and among its agents, if any, by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Company to comply with its legal obligations.

b. The legislation and Regulatory directives places responsibility upon MAAFIN, its employees and its agents to combat money laundering and covers a very wide area of financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime. It applies to all employees involved in handling monetary transactions. It is a criminal offence to, assist a money launderer, "tip off" a person suspected to be involved in money laundering that they are suspected or that they are the subject of police investigations, fail to report a suspicion of money laundering and acquire, use, or possess criminal property.

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

Gold Loan including all types (online or offline)
Vehicle and Equipment Finance
All other businesses/products/services such as: -

- ➔ SME Loans

- ➔ Secured Personal Loan
- ➔ Micro SME Loan

d. Any other activities requiring onboarding of a customer, whether corporate or otherwise, for the purpose of any one off or continued transactions.
e. Anywhere applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India. RBI may advise further necessary action by the MAAFIN including application of additional measures to be taken to manage the money laundering or terror funding risks.

This Policy shall be reviewed annually or as and when the Board deems it fit to review..

5. Definitions

a. Beneficial Owner (BO)

- ➔ 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.

  "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
  "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 shareholder's agreements or voting agreements.

- ➔ 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 or who exercises control through other means.

  Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

- ➔ 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.

➔ 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% 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.

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

C. "Customer "means.

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

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

d. "Digital KYC" means 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 authorized officer of the Regulated Entity (RE) as per the provisions contained in the Act.

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

f. "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.

g. "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.

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

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

j. "Obtaining certified copy of Officially Valid Document (OVD)" – Means comparing the copy of OVD with the original and recording the same on the copy by authorized employer of the Company. 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 of OVD, certified by any one of the following, may be obtained:

- ➔ authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
- ➔ branches of overseas banks with whom Indian banks have relationships,
- ➔ Notary Public abroad,
- ➔ Court Magistrate,
- ➔ Judge Indian Embassy/Consulate General in the country where the non-resident Customer resides.

k. "Offline verification" means the process of verifying the identity of the Aadhaar

number holder without authentication, through such offline modes as per clause (pa) of paragraph 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

l. "Senior Management"

Senior Management for the purpose of the Policy shall constitute MD, CEO, Chief Financial Officer, GM (Credit), CCO, CRO, Company Secretary, Business Head of Gold Loan Department.

.

m. "Video based Customer Identification Process (V-CIP)": an alternative method of customer identification with facial recognition and customer due diligence by an authorized official of the RE 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 Master Direction.

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

6. Customer Due Diligence (CDD)

a. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

i. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable.
ii. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control.
iii. Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification

b. "Designated Director" means the Managing Director to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

c. "Person" has the same meaning assigned in the Act and includes:

i. an individual,
ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. v.an association of people or the body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons
vii. (i to v), and
viii. any agency, office or branch owned or controlled by any of the above persons (i to vi).

d. "Non-profit organization" means which will now include any entity or organization

constituted for religious or charitable purposes referred to in Paragraph 2(15) of the Income- tax Act, 1961; or registered as a trust or a society under the Societies Registration Act, 1860 or any similar state legislation; or a company registered under Paragraph 8 of the Companies Act, 2013.

e. 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:

- ➔ 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
- ➔ appears to be made in circumstances of unusual or unjustified complexity; or
- ➔ appears to not have economic rationale or bona-fide purpose; or
- ➔ gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

f. Transaction" means purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- ➔ opening of an account.
- ➔ deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means.
- ➔ the use of a safety deposit box or any other form of safe deposit.
- ➔ entering any fiduciary relationship.
- ➔ any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- ➔ establishing or creating a legal person or legal arrangement.

g. "Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

h. Simplified Due Diligence (SDD) - MAAFIN may apply Simplified Due Diligence measures in respect of customers classified as Low Risk, based on its risk assessment framework, in accordance with RBI Master Direction – KYC, 2025.

SDD may be applied subject to the following conditions:

- Customer is classified as Low Risk based on risk categorization parameters.

- There is no suspicion of money laundering or terrorist financing.
- Customer identity and address are verified through reliable sources.
- The nature of business relationship presents minimal ML/TF risk.
- Ongoing monitoring of such accounts shall continue.

SDD shall not be applied where:

- Customer is classified as Medium or High Risk
- Suspicious activity is observed
- Customer is Politically Exposed Person (PEP)
- Non face-to-face onboarding without additional safeguards

The decision to apply SDD shall be documented and subject to periodic review.

7.Key Elements of The Policy

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

The Policy includes the following key elements:

7.1 Customer Acceptance Policy (CAP)
7.2 Customer Identification Procedures (CIP)
7.3 Monitoring of Transactions (including Reporting STR, CTR & CCR)
7.4 Risk Management

7.1 Customer Acceptance Policy (CAP)

The Company's CAP lays down criteria for acceptance of Customers. while taking decision to grant any facilities to the Customers as well as during the continuation of any facilities, the following norms and procedures shall be followed by the company

- ➔ No account will be opened in anonymous or fictitious/benami name.
- ➔ Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks will be done before opening a new account to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities.
- ➔ MAAFIN will refrain from opening an account where the company 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 shall be undertaken without the Customer Due Diligence procedure (CDD), set out in para 6.3 of the RBI Master Direction on KYC. CDD procedures to be followed for all joint account holders while opening joint accounts.
- ➔ A Unique Customer Identification Code (UCIC) shall be allotted to new and existing Customers. MAAFIN shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant Customer of MAAFIN desires to open another account with MAAFIN, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
- ➔ MAAFIN has a system 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, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- ➔ MAAFIN shall ensure to specify the mandatory information which need to be sought for KYC purpose while opening an account and during the periodic updation.
- ➔ MAAFIN shall ensure the optional /Additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer after the account is opened. Circumstances in which a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- ➔ Where Goods and Services Tax (GST) details are available the GST number shall be verified from the search/verification facility of the issuing authority.
- ➔ Where MAAFIN is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR

The implementation of CAP should not become too restrictive and result in denial of the MAAFIN's services to the public, especially those who are financially or socially disadvantaged.

7.2 Customer Identification Procedure (CIP)

a. Customer Identification involves verification of Customer's identity by using reliable, independent source documents, data, or information. MAAFIN shall obtain enough information necessary to verify the identity of each Customer. A broad guideline for Customer identification is given below:

- ➔ MAAFIN shall ensure that the Customer identification process is undertaken, whenever, an account-based relationship is being established.
- ➔ carrying out any international money transfer operations for a person who is not an account holder.
- ➔ there is doubt about the authenticity or adequacy of Customer identification data already obtained.
- ➔ selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
- ➔ carrying out transactions with walk in Customers, where the amount involves equal or exceeds rupees fifty thousand, whether conducted as a single transaction or
- ➔ several transactions that appear to be connected.
- ➔ MAAFIN has reasons to believe that a Customer is intentionally structuring transactions into a series of transactions below the threshold of Rupees Fifty thousand.
- ➔ MAAFIN shall also ensure that introduction is not to be sought while opening accounts.

b. VIDEO BASED CUSTOMER IDENTIFICATION PROCESS (V-CIP):

i. MAAFIN may undertake live V-CIP for establishment of an account-based relationship with an individual Customer after obtaining his informed consent and adhering to the procedures prescribed in RBI regulations. This process shall be treated as face-to-face process for the purpose of Customer identification.

The officials performing the V-CIP shall record video as well as capture photograph of the Customer present for identification and obtain the identification information as below:

- ➔ 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.
- ➔ Live location of the Customer (Geo tagging) shall be captured to ensure that Customer is physically present in India.
- ➔ The official shall ensure that photograph of the Customer in the Aadhaar/PAN details matches with the Customer undertaking the V-CIP and the dentification details in Aadhaar/PAN shall match with the details provided by the Customer.
- ➔ The official shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

- ➔ In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.
- ➔ All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.
- ➔ It shall be ensured that the process is a seamless, real-time, secured, end-to- end encrypted audio-visual interaction with the Customer and the quality of the communication is adequate to allow identification of the Customer beyond doubt. MAAFIN shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.
- ➔ To ensure security, robustness and end to end encryption, MAAFIN shall carry out software and security audit and validation of the V-CIP application before rolling it out.
- ➔ . The audio-visual interaction shall be triggered from the domain of MAAFIN and not from third party service provider, if any. The officials operating the V-CIP process shall be specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.
- ➔ The video recording shall be stored in a safe and secure manner and bears the date and time stamp.
- ➔ It shall be ensured that the Aadhaar number is redacted or blacked-out

c. CIP Infrastructure

The Company 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 Company 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. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company's 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 Company.

- ➔ The Company 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.

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

- 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.

- 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 Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

- Based on experience of detected / attempted / 'near-miss cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

- The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

- The V-CIP application software and relevant APIs / web services 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.

d. V-CIP Procedure

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

e. Customer Due Diligence Procedure (CDD) In Case of Individuals

- Before obtaining KYC documents from the customer, the Company shall first seek the KYC Identifier and retrieve the customer's KYC records from CKYCR. Where the KYC records are successfully retrieved and found to be complete and up-to-date, the Company shall not insist on submission of fresh KYC documents, unless required for verification, updation or enhanced due diligence, as per RBI KYC Directions

- For undertaking CDD, MAAFIN shall obtain the following from an individual while establishing an account-based relationship or while dealing with an

individual who is a beneficial owner, authorised signatory or power of attorney holder related to any legal entity. The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder. Submission of Aadhaar for KYC purposes shall be strictly voluntary. If the customer does not wish to submit Aadhaar, the Company shall accept any other Officially Valid Document (OVD) as prescribed under RBI KYC Directions. No customer shall be denied any service or facility solely on the ground that Aadhaar has not been submitted.

- A certified copy of Officially Valid Documents (OVD), as given in Annexure I.
- One recent photograph (For the gold loan Customers capturing of photos of the individuals and keeping in the ERP to be continued).
- Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1961; and such other documents pertaining to the nature of business or financial status specified in this Policy.

f. Offline Verification Through Proof of Possession of Aadhaar Number:

➔ MAAFIN may carry out Offline Verification of Customers if they are desirous of undergoing Aadhaar Offline Verification for identification purposes. No such offline verification shall be performed without obtaining the written consent of the Customer in the manner prescribed in the Aadhaar Regulations.

➔ 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.

➔ Wherever Aadhaar details are collected, it shall be ensured that Customers have redacted or blacked out their Aadhaar numbers through appropriate means. The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification, when NBFCs or itself are authorized by RBI to do such verification for establishing account-based relationship.

g. Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode

MAAFIN shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. MAAFIN has a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

h. Verification Through Digital KYC:

MAAFIN may carry out verification by capturing live photo of the Customer and OVD or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with latitude and longitude of the location where such live photo is being taken by the authorized officer of the Company.

i. Verification of Equivalent E-Document:

Where the Customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the Customer, MAAFIN shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the Customer as specified in the guidelines for digital KYC.

j. 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 to verify his/her identity shall be undertaken keeping in view the following:

Where the Customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) 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.
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.

k. CDD MEASURES IN RESPECT OF NON-INDIVIDUALS:

CDD Standards and documents to be collected in respect of Proprietary firms, partnership firms, companies and other Legal entities are given in Annexure I.

l. CUSTOMER DUE DILIGENCE BY THIRD PARTY

- ➔ In compliance of the KYC regulations, MAAFIN may rely on the Customer due diligence done by third parties, for verifying identity of Customers at the time of commencement of account-based relationship, subject to the following conditions.

- ➔ Records or information of the Customer due diligence carried out by the third

party is obtained immediately from the third party or from Central KYC Records Registry.

- ➔ MAAFIN 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.

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

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

- ➔ The ultimate responsibility for Customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with MAAFIN. (Description of RE are given in Annexure II).

m. MAAFIN shall ensure compliance with KYC Policy through:

- ➔ Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
- ➔ Allocation of responsibility for effective implementation of policies and procedures
- ➔ at HO / Branch level.
- ➔ Independent evaluation of the compliance functions of REs' policies and procedures, including legal and regulatory requirements.
- ➔ Concurrent/internal audit system to verify compliance with KYC/AML policies and procedures.
- ➔ Submission of quarterly audit notes and compliance to the Audit Committee.

- ➔ MAAFIN shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

7.3 Monitoring of Transactions

a. Monitoring

- ➔ MAAFIN shall monitor transactions on an ongoing basis for the purpose of reporting it to the appropriate authorities in case any suspicious transactions are found to be carried out by the concerned Customer. (An illustrative list of suspicious transactions is given in Annexure III). The extent of monitoring by the MAAFIN will depend on the risk sensitivity of the account and special attention will be given to all complex unusually large transactions, which have no apparent economic or lawful purpose.
- ➔ MAAFIN shall exercise caution with respect to the transactions with persons (including legal persons and other financial institutions) from the countries which

have been identified by Financial Action Task Force (FATF) as high risk and non-cooperative jurisdictions with respect to compliance with the FATF Recommendations, 2012.

- ➔ Transactions carried out involving Jurisdiction and countries that do not or insufficiently apply the FATF recommendations like the FATF Grey List countries
- ➔ ,i.e., those countries that are subject to increased monitoring as a result of their AML/CFT deficiencies and the Black Listed countries, i.e., those countries that FATF has deemed to have "significant strategic deficiencies" in their AML/CFT regimes shall be subject to additional monitoring.
- ➔ FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. REs shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
- ➔ Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

- ➔ The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

  MAAFIN shall file Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling under FATCA in terms of the direction of the RBI/PMLA in respect of all products/ services.

b. Ongoing Due Diligence

i. MAAFIN 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 source of funds/wealth.
ii. Without prejudice to the generality of factors that call for close monitoring, the following types of transactions are monitored closely: -

- ➔ 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.
- ➔ Transactions which exceed the thresholds prescribed for specific categories of accounts.
- ➔ High account turnover is inconsistent with the size of the balance maintained.
- ➔ Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
- ➔ The extent of monitoring shall be aligned with the risk category of the Customer and

high-risk category accounts shall be subjected to more intensified monitoring.

➔ A system of periodic review of risk categorization 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.

7.4 Risk Management

a. Monitoring of Risk Management

➔ Risk categorization of Customers shall be undertaken based on various factors, such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, 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 MAAFIN has categorized its customers into 'High Risk / Medium Risk / Low Risk' based on the profile of the Customers. MAAFIN shall apply higher due diligence measures keeping in view the risk level.

➔ MAAFIN has developed robust underwriting procedures for onboarding borrowers, which include verification of ownership of the gold ornaments (in the case of gold loans), assessment of financial resources of the borrowers, collection of their market reports etc. (for other loans).

➔ MAAFIN's internal audit periodically evaluates the level of adherence to the KYC procedures. Audit function should provide an independent evaluation of the effectiveness of KYC policies and procedures, including legal and regulatory requirements.

➔ The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

b. Risk Assessment

➔ MAAFIN shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, cognizance of the overall sector-specific vulnerabilities if any, that the regulator/supervisor may share from time to time shall be taken.

➔ The risk assessment exercise shall be conducted on a half yearly basis and parameters of the assessment shall be modified, in alignment with the outcome of the risk assessment exercise. An internal document detailing the assessment process may be kept separately for the same.

➔ The outcome of the exercise shall be put up to Risk Management Committee and should be available to competent authorities and self-regulating bodies.

➔ MAAFIN shall carry out sanctions screening based on the consolidated list of the RBI. The department shall update the list at periodical intervals. Such screening will be carried out automatically/manually of all Customers at the time of onboarding. MAAFIN shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall monitor the implementation of the controls and enhance them, if necessary.

➔ The Company is encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

C. Periodic Updation

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 as per the following procedure.

i. For Individual Customers

➔ 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 the MAAFIN, Customer's mobile number registered with the MAAFIN, digital channels (such as mobile application of MAAFIN), letter etc.

➔ 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 the MAAFIN, Customer's mobile number registered with the MAAFIN, digital channels (such as mobile application of MAAFIN), 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, MAAFIN, may at its option, obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as mentioned in Annexure 1, for the purpose of proof of address, declared by the Customer at the time of periodic updation.

➔ 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. MAAFIN shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, to prevent any fraud.

ii. Customers Other Than Individuals

- ➔ No change in KYC information: In case of no change in the KYC information of the LE Customer, a self-declaration in this regard shall be obtained from the LE Customer through its email id registered with MAAFIN, digital channels (such as mobile application of MAAFIN), letter from an official authorized by the LE in this regard, board resolution etc. Further, MAAFIN shall during this process ensure that the Beneficial Ownership (BO) information available is accurate and shall update the same, if required, to keep it as up- to-date as possible.
- ➔ Change in KYC information: In case of change in KYC information, MAAFIN shall undertake the KYC process equivalent to that applicable for on- boarding a new LE Customer.
- ➔ ADDITIONAL MEASURES: In addition to the above, MAAFIN shall also ensure that,

- ➔ The KYC documents of the Customer as per the current CDD standards is available and this shall be applicable even if there is no change in Customer information but the documents available with the MAAFIN are not as per the existing CDD standards. Further, in case the validity of the CDD documents available with MAAFIN has expired at the time of periodic updation of KYC, MAAFIN shall undertake the KYC process equivalent to that applicable for on- boarding a new Customer.
- ➔ Customer's PAN details, if available with the MAAFIN, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- ➔ An 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.
- ➔ In order to ensure Customer convenience, MAAFIN may consider making available the facility of periodic updation of KYC at any of its branches.
- ➔ MAAFIN shall adopt a risk-based approach with respect to periodic updation of KYC.
- ➔ MAAFIN shall advise the customers that 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; MAAFIN will collect the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at MAAFIN's end

  (Note: The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.)

iii. Existing Customers

- ➔ For gold loan Customers, a copy of the PAN Card of the borrower shall be collected for all transaction above 5 lakhs as guided by the regulatory guidelines to NBFCs financing against the collateral of gold.

iv. Simplified norms for Self Help Groups (SHGs)

- ➔ CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs.

Reporting Requirements to Financial Intelligence Unit – India

REs shall not put any restriction on operations in the accounts where an if has been filed. REs shall keep the fact of furnishing of STR strictly confidential

MAAFIN has put in place appropriate procedures to ensure effective implementation of KYC guidelines.

d. Enhanced Due Diligence

i. Company shall, prior to the commencement of each specified transaction, —

➔ verify the identity of the clients undertaking such specified transaction by

➔ authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (18 of 2016) in such manner and subject to such conditions, as may be prescribed:

➔ Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed;

➔ take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed;

➔ take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

ii. Where the client fails to fulfill the conditions laid down under sub-paragraph (1), the reporting entity shall not allow the specified transaction to be carried out.

iii. Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed. The opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." MAAFIN shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND.

The information obtained while applying the enhanced due diligence measures under sub-paragraph (1) shall be maintained for a period of ten years from the date of transaction between a client and the reporting entity.

Explanation. —For the purposes of this paragraph, "specified transaction" means—

- ➔ any withdrawal or deposit in cash, exceeding such amount.
- ➔ any transaction in foreign exchange, exceeding such amount; any transaction in any high value imports or remittances.
- ➔ such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

e. Accounts of Politically Exposed Persons (PEP):

Politically Exposed Persons are those 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/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

Special care and diligence shall be taken in respect of Politically Exposed Persons. Generally, the MAAFIN may not (would not) open loan accounts of PEP. However, any request from PEPs shall be escalated to Senior Management and will be dealt with based on their approval and will be subject to enhanced due diligence (comprising of additional documents) and monitoring.

- ➔ sufficient information including information about the sources of funds, accounts of family members and close relatives is gathered on the PEP;
- ➔ the identity of the person shall have been verified before accepting the PEP as a customer.
- ➔ the decision to open an account for a PEP is taken at a senior level in accordance with the MAAFIN Customer Acceptance Policy.
- ➔ all such accounts are subjected to enhanced monitoring on an on-going basis;
- ➔ 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.
- ➔ the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner, to family members or close relatives of PEP.

f. Accounts of Non-Face-To-Face Customers:

These Customers are those who opened accounts without visiting the branches / offices of MAAFIN or meeting its officials. MAAFIN shall ensure that first payment from these accounts shall be affected through the Customers' KYC-Complied account with another Regulated Entity.

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than

customer onboarding in terms of Paragraph 17):

Non-face-to-face onboarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non- face-to-face modes for the purpose of this Paragraph includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non- digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by REs for non-face-to-face customer onboarding (other than customer onboarding in terms of Paragraph 17):

- ➔ In case of the Company introducing the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- ➔ 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.
- ➔ Apart from obtaining the current address proof, RE shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- ➔ The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- ➔ First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- ➔ 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.

g. Client Accounts Opened by Professional Intermediaries:

- ➔ MAAFIN shall ensure while opening client accounts through professional intermediaries that:
- ➔ Clients shall be identified when the client account is opened by a professional intermediary on behalf of a single client.
- ➔ MAAFIN shall have the option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- ➔ MAAFIN shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details

to MAAFIN.

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

MAAFIN may, at its 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.

The ultimate responsibility for knowing the Customer lies with MAAFIN.

h. Confidentiality of Information About Customers

All the information collected from the Customers by MAAFIN shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the Customers. Additionally, the information sought from each Customer should be relevant to the risk perceived in respect of that Customer, should not be intrusive and should be in line with the guidelines issued by the RBI in that behalf.

Information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Exception to the confidentiality of customer information shall be as under:

- ➔ Where disclosure is under compulsion of law.
- ➔ Where there is a duty to the public to disclose.
- ➔ The interest of the company requires disclosure.
- ➔ Where the disclosure is made with express or implied consent of the customer.

I. Maintenance of Records of Transactions

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

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

iii. preserve the records pertaining to the identification of the Customers and their addresses obtained while opening the account and during business relationship, for at least ten years after the business relationship is ended or the account has been closed, whichever is later.

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

v. 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)

vi. maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit reconstruction of individual transactions, include following:

- ➔ the nature of the transactions.
- ➔ the amount of the transaction and the currency in which it was denominated.
- ➔ the date on which the transaction was conducted; and
- ➔ the parties to the transaction.

vii. MAAFIN have a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

viii. Maintain records of the identity and address of its customers, and records in respect of transactions referred to in Rule 3 of PML Rules, in hard or soft format.

Explanation. – For the purpose of this Paragraph, 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 MAAFIN shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, MAAFIN shall register the details on the DARPAN Portal. MAAFIN shall also maintain such registration records for a period of ten years after the business relationship between the customer and the MAAFIN has ended or the account has been closed, whichever is later.

8.General

i. Adherence to KYC Guidelines by Agents/ Brokers or The Like

Agents/ brokers or the like shall be appointed only after detailed due diligence and ensuring that they are fully compliant with KYC guidelines applicable to MAAFIN.
MAAFIN shall make available all information to RBI to verify the compliance with KYC guidelines. MAAFIN shall be responsible for non-customer guidelines by the brokers/agents etc. who are operating on MAAFIN's behalf.

ii. Principal Officer

MAAFIN shall have a designated Principal Officer (PO) who shall be responsible for ensuring compliance, monitoring transactions, sharing, and reporting information as required under the law/regulations and responsible for furnishing information as per

rule 8 of the Rules. The Chief Compliance Officer of MAAFIN shall be the Principal Officer.

iii. Designated Director

MAAFIN shall have a Designated Director, to ensure overall compliance with the obligations under the Prevention of Money laundering Act, 2002 and Rules framed thereunder, from time to time. The Managing Director of MAAFIN shall be the Designated Director.

The name, designation and address of the Principal Officer and the Designated Officer shall be communicated to the FIU-IND and to the RBI.

iv. Staff and Management Responsibilities – Offence of Money Laundering

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

v. CDD Procedure and Sharing KYC Information with Central KYC Records Registry (CKYCR)

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

MAAFIN shall also ensure that during periodic updation of the Customers, the Customers are migrated to the current CDD standard as applicable to MAAFIN.
Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.
MAAFIN shall ensure to capture customers' KYC records and upload them onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
In Rule 9(1C) of the PML Rules, the MAAFIN shall ensure within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR

"KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities. The templates may be revised from time to time, as may be required and released by CERSAI.

Once KYC Identifier is generated by CKYCR, Company shall ensure that the same is communicated to the individual/LE. additionally, Company ensures that during periodic updation, the customer is migrated to the current CDD standard.

Where a customer, For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–
there is a change in the information of the customer as existing in the records of CKYCR; or
the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
the validity period of downloaded documents has lapsed; or
the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

Vi. **Training Program**

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

9.Compliance With Policy Norms

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

10.Other Operating Instructions

- In case of Customers whose accounts have not been operated (or who have not been transacting) for more than 12 months, fresh KYC documents will need to be taken before undertaking any new transactions. System based control will be put in place.

➔ As a Policy, Gold loan will be granted to individuals only and not to companies, firms, trusts etc.

➔ In the case of 'pardanashin' (veil) women, capturing of the customer's photograph (in Customer ID file on the system) may waived provided an acceptable Proof of Identity document is furnished and KYC verification has been carried down by any of female staffs.

11.Other Obligations

a. under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

i. The Company shall ensure meticulous compliance with the "Procedure for Implementation of Paragraph 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Paragraph 12A of the WMD Act, 2005 vide Order dated January 30, 2023, or any latest amendments updated by the Ministry of Finance, Government of India.

ii. In accordance with paragraph 3 of the aforementioned Order, The Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

iii. Further, REs shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

iv. In case of match in the above cases, The Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Paragraph 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. REs shall file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

v. REs may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

vi. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-paragraph (2) of Paragraph 12A of the WMD Act, 2005, The Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

vii. In case an order to freeze assets under Paragraph 12A is received by the Res from the CNO, REs shall, without delay, take necessary action to comply with the Order.

viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by RE along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

ix. The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, REs shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Paragraph 51A of the UAPA and Paragraph 12A of the WMD Act.

The Company shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

b. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967

All offices shall ensure that in terms of Paragraph 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals / entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

i. The "ISIL (Da'esh) & Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/fop/fopxml=htdocs/resources/xml/en/consolidated.xml &xslt=htdocs/resou rces/xsl/en/al-qaida-r.xsl

ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/fop/fopxml=htdocs/resources/xml/en/consolidated.xml &xslt=htdocs/resou rces/xsl/en/taliban-r.xsl.

All offices shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by all the offices for meticulous compliance.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required

under UAPA notification dated February 2, 2021 (Annex II of (Annex II of Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on January 04, 2024).

Freezing of Assets under Paragraph 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on January 04, 2024), shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

Annexure I

CDD & OFFICIALLY VALID DOCUMENTS (OVD)

1.Individuals

Officially Valid Documents (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the voters 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,

a. 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.
b. where the OVD furnished by the Customer does not have updated address, the following documents 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.
    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 license agreements with such employers allotting official accommodation.

C. The Customer shall submit OVD with current address within a period of three months of submitting deemed OVDs

d. 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.

Non-Individuals (Companies, Firms, Trusts etc.)

KYC norms are applicable to non-individuals also. The requirements are as under.

Legal entities (Companies)	Certified copies of each of the following documents shall be obtained: a. Certificate of incorporation with Memorandum & Articles of Association b. Resolution of Board of Directors for opening the account and Power of Attorney / authorization of persons to operate the account on its behalf c. PAN allotment letter/ PAN of the Company d. Documents as specified in para 1 above of the individuals holding attorney /authorization to transact on company's behalf. e. CDD of the Individual beneficial owner as detailed in para 6.3 f. the names of the relevant people holding senior management position; and g. the registered office and the principal place of its business, if it is different

Partnership Firms	Certified copies of each of the following documents shall be obtained: Registration certificate. Partnership deed. PAN of the partnership firm Documents as specified in para 1 above of the individuals holding attorney /authorization to transact on its behalf. the names of all the partners and address of the registered office, and the principal place of its business, if it is different.

Proprietary firms	For opening an account, CDD of the individual (proprietor) as mentioned in para 6.3 shall be carried out PLUS any two of the below mentioned documents, Registration certificate including Udyam Registration Certificate (URC) Certificate/License issued under Shops & Establishment Act GST and Income Tax returns GST registration certificate (provisional/ final) Utility bills such as electricity, water, telephone bills etc. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. IEC (Import Export Code) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. In cases where the MAAFIN is satisfied that it is not possible to furnish two such documents, MAAFIN may, at its discretion, accept only one of those documents as proof of business/activity. Provided MAAFIN shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Trusts	Certified copies of each of the following documents shall be obtained: Certificate of Registration; Trust Deed Power of Attorney authorizing a person to carry out transactions on behalf of the trust Permanent Account Number or Form No.60 of the trust; and such documents as are required for an individual under sub-rule (1) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf the names of the beneficiaries, trustees, settlor, protector and authors of the trust and the address of the registered office of the trust; and list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust.
Any unincorporated association or a body of individuals	For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents 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 Para 1, of the person holding an attorney to transact on its behalf and Such information as may be required by MAAFIN to collectively establish the legal existence of such an association or body of individuals.

Juridical persons not specifically covered in the earlier part, such as societies, universities, and local bodies like village panchayats	For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents shall be obtained: (a) Document showing name of the person authorised to act on behalf of the entity. (b) Documents, as specified in Para 1, of the individual holding an attorney to transact on its behalf and (c) Such documents as may be required by MAAFIN to establish the legal existence of such an entity/juridical person.

Annexure II

a. Regulated Entities:

b. All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licensed under Paragraph 22 of Banking Regulation Act, 1949.

c. All India Financial Institutions (AIFIs).

d. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

e. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

f. All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

g. Depository Participant (DP) service

Annexure III

Illustrative 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

a. False identification documents
b. Identification documents which could not be verified within reasonable time
c. Accounts opened with names very close to other established business entities.

2.Background Of Client

Suspicious background or links with known criminals.

3.Multiple Accounts

Large number of accounts having a common account holder, introducer, or authorized personnel.

4.Signatory With No Rationale

. Unexplained transfers between multiple accounts with no rationale.

5.Activity In Accounts:

a. Unusual activity compared with past transactions- Sudden activity in dormant accounts;
b. Activity inconsistent with what would be expected from declared business.

6.Nature Of Transactions:

a. Unusual or unjustified complexity.

b. No economic rationale or bonafide purpose.

c. Frequent cash transactions.

d. Nature of transactions inconsistent with what would be expected from declared business.

7.Value Of Transactions:

a. Value just under the reporting threshold amount in an apparent attempt to avoid reporting.

b. Value inconsistent with the client's apparent financial standing.

8.Indicators Of Suspicious Transactions:

a. Reluctant to part with information, data, and documents.

b. Submission of false documents, purpose of loan and detail of accounts.

c. Reluctance to furnish details of source of funds.
d. Reluctance to meet in person, representing through power of attorney.

e. Approaching a distant branch away from own address.

f. Maintaining multiple accounts without explanation.

g. Payment of initial contribution through unrelated third-party account.

h. Suggesting dubious means for sanction of loan.

i. Where transactions do not make economic sense.

j. Where doubt about beneficial ownership.

k. Encashment of loan through a fictitious bank account.

l. Sale consideration quoted higher or lower than prevailing prices.

m. Request for payment in favor of third party with no relation to transaction.

n. Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent.
o. Frequent request for change of address.

p. Over-payment of instalments with a request to refund the overpaid amount

Annexure IV

Digital KYC Process (RBI Guidelines)

a. The RE 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 REs.

b. The access of the Application shall be controlled by the REs 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 REs to its authorized officials. C. The Customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the Customer.

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

d. The Application of the RE 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.

e. 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 watermarking 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.

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

g. 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.

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 the authorized officer registered with the RE shall not be used for Customer signature. The RE must check that the mobile number used in Customer signature shall not be the mobile number of the authorized officer.

h. 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 RE. 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.

i. After all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE and 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.

j. The authorized officer of the RE shall check and verify that:- (i) information available in the picture of document matches 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.

k. On Successful verification, the CAF shall be digitally signed by authorized officer of the RE 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.