KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEYLAUNDERING POLICY

Version Control		
Version Number	**Description**	**Date**
Version 0.1	Modification of existing Policy	Aug 2019
Version 0.2	Amendment	July 2020
Version 0.3	Renewal	July 2021
Version 0.4	Renewal	July 2022
Version 0.5	Renewal	July 2023
Version 0.6	Renewal	Oct 2024
Version 0.7	Amendment	Nov 2024
Version 0.8	Amendment	Oct 2025

Effective Date	30 October 2025
Next Review Date	October 2026
Policy Owner	Operations Department
Prepared By	Operations Department
Reviewed by	Policy Review Committee
Approved By	Board of Directors

1. INTRODUCTION

Reserve Bank of India (RBI) with the objective to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system as part of the efforts continuously being made both internationally and nationally, has been prescribing various rules and regulations by way of its Master Directions – Know your Customer (KYC) Directions from time to time for all Regulated entities (REs) to comply. The latest comprehensive directions were re issued on 06th November, 2024 after incorporating all the amendments (Master Direction DBR.AML.BC.No.81/14.01.001/2015-16), updated as on 14th August 2025.

Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

Statutory background

Besides RBI directions there are certain statute related requirements that are also required to be complied with by Manappuram Finance Limited (hereinafter referred to as "MAFIL" or "the Company") in its conduct of operations. It includes Prevention of Money-Laundering Act, 2002 ("PML Act"), Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), amended from time to time and Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (as amended as on 2nd February 2021). In addition, being a listed entity, MAFIL is required to comply with the relevant norms as put out by SEBI relating to Anti Money Laundering (AML) standards to be followed by market intermediaries viz Depository Participants, Asset Management Companies etc. Accordingly, MAFIL puts in place the Policy, which is further detailed below:

FAQ on KYC can be accessed through the RBI website using the path below;
www.rbi.org.in >> more links >> FAQs >> FAQs on Master Directions on KYC

In observance of these directions MAFIL has put in place a detailed policy and procedures (SOPs) to guide and enable its day-to-day operations. Details are detailed herein below

2. POLICY STATEMENT

MAFIL 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. MAFIL 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 activities of the Company. 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, money laundering, 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 PML Act.

3. OBJECTIVES OF THE POLICY:

The Policy seeks to achieve the following objectives.

- To provide a framework for how the company, in its process of conducting business with Customers, will deal with the threat of money laundering and terrorism financing.
- To prevent criminal elements from using the Company for Money Laundering and Terrorist Funding activities.
- To ensure that all the staffs are aware and receive training on the Anti Money laundering legislation applicable to them, as well as to adhere to their responsibilities under the regulations.
- To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
- To enable the Company to know and understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities as envisaged under the PML Act and in accordance with laid down procedures.
- To comply with applicable laws and regulatory guidelines

4.SCOPE OF THE POLICY

This Policy applies to all the employees of MAFIL 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.

The legislation and Regulatory directives places responsibility upon MAFIL, 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 with 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.

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 MAFIL 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
- Remittances (Pay out of Inward remittances from abroad under MTSS)
- Issuance of Pre-paid Instruments.
- Depository Account services
- Money Changing as a Full-Fledged Money changer (FFMC)
- All other businesses/products/services such as: -
    a) Digital Personal Loan
    b) Health Care Industry Loan
    c) Micro Home Finance
    d) MSME
    e) Secured Personal Loan
    f) Corporate Loans
    g) Loan to Consumer Durables
    h) Loan to Food Industry
    i) Mahila Credit Loan
    j) Micro Credit Loan
    k) Restaurant Finance
    l) School Finance
    m) Small Scale Industrial Finance
    n) Traders Micro Credit
- Any other activities requiring on boarding of a customer, whether corporate or otherwise, for the purpose of any one-off transactions or continued account-based transactions.

This Policy shall be reviewed annually by the Board of Directors.

5.IMPORTANT DEFINITIONS

(i) **Beneficial Owner (BO)**

a. 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-
"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.

b. 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.

c. 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.

d. 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.

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

(iii) "**Customer**" means

a. a person who is engaged in a financial transaction or activity with MAFIL and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.
b. any other person connected with a financial transaction which can pose significant reputation or other risks to MAFIL.

(iv) "**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:

a. 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.
b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control.
c. 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.

(v) "**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

(vi) "**Designated Director**" means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013..

(vii) "**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 PML Act.

(viii) "**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 section (3) of the Information Technology Act, 2000.

(ix) "**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.

(x) "**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.

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

(xii) "**Non-face-to-face Customers**" means Customers who open accounts without visiting branches / offices of MAFIL or meeting its officials.

(xiii) **"Non-profit organization"** means any entity or organization constituted for religious or charitable purposes referred to in Section 2(15) of the Income-tax Act, 1961; 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.

(xiv) "**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,

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 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;
    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 the documents specified at 'b' above
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.

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.

(xv) "**Obtaining certified copy of Officially Valid Document (OVD)**" means comparing the copy of OVD with the original and recording the same on the copy by authorized officer of MAFIL. 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.

(xvi) "**Offline verification**" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the regulations made by the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

(xvii) "**Person"** has the same meaning assigned in the Act and includes:

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e),and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

(xviii) "**Senior Management**" for the purpose of the Policy shall constitute Managing Director & Chief Executive Officer, Chief Financial Officer, Head - Analytics and Business Review, Company Secretary, Vice President – Compliance Head, Chief Compliance Officer, Chief Risk Officer, Head - Information Technology Department, Head - Human Resource Department, Head - Internal Audit Department, Head - Human Resource Management Training Department, Head - Operation Department, Head - Vigilance Department, Business Head - Gold Loan Department.

(xix) "**Suspicious transaction**" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. 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
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. 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.

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

a. opening of an account;
b. 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;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

(xxi) "**Video based Customer Identification Process (V-CIP)**" is an alternative method of customer identification with facial recognition and customer due diligence by an authorized official of the Company by undertaking seamless, secure, live, informed consent-based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence (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 Customer Identification Purpose (CIP).

(xxii) "**Walk-in Customer**" means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.

(xxiii) "**Wire transfer**" related definitions:

a. Batch transfer: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.
b. Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
c. Beneficiary RE: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary RE and makes the funds available to the beneficiary.
d. Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
e. Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
f. Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
g. Financial Institution: In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
h. Intermediary RE: Intermediary RE refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
i. Ordering RE: Ordering RE refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request fora wire transfer on behalf of the originator.
j. Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
k. Serial Payment: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).
l. Straight-through Processing: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.
m. Unique transaction reference number: Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
n. Wire transfer: Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the PML Act, the PML Rules, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6.GENERAL PROVISIONS OF THE POLICY:

6.1 Policy to be approved by the Board

In accordance with the Master Directions issued by the RBI, MAFIL is required to put in place a Know Your Customer (KYC) policy duly approved by the Board of Directors of the Company.

6.2 Requirement of Group wide policy

In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act. As of now MAFIL has four subsidiaries and in pursuance of the PML Rules, it becomes necessary for the Company to formulate and implement a group wide program 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 with adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

While 2 subsidiaries are regulated by RBI and is required to comply with the Master Directions of RBI on this subject. MAFIL as the parent Company shall put in place a policy with base line requirements as required covering all the group entities.

The policy shall also adopt the best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

7 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY MAFIL:

MAFIL shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically, at quarterly intervals to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment report the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

The Company shall carry out the risk assessment proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of its operations and shall be documented appropriately. Further, the periodicity (at least quarterly) of risk assessment exercise shall be determined by the Board in alignment with the outcome of the risk assessment exercise.

MAFIL shall submit the outcome of the exercise to the Board and shall be made available to competent authorities and self-regulating bodies.

As part of compliance program for KYC/AML, the Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified by MAFIL or through national risk assessment) and shall put in place Board approved policies, controls and procedures in this regard. The Company shall implement CDD procedures/programs, having regard to the ML/TF risks identified and the size of business. Besides, MAFIL shall monitor the implementation of the controls and enhance them if necessary.

7.1 Designated Director:

In accordance with the Master Direction, the Board is required to nominate a person to be designated as a person to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act. The nominated Director is required to be an officer other than the Principal Officer nominated as detailed in below;

The name, designation, address and contact details of the Designated Director is required to be communicated to the FIU-IND and also to the RBI.

MAFIL's Board has nominated Managing Director of the Company as the "Designated Director" and the corresponding details have been communicated to RBI. MAFIL shall ensure to communicate any change in the name and details of the Designated Director to FIU- IND and RBI whenever it occurs.

7.2.Principal Officer:

The Master Direction also requires MAFIL to nominate a "Principal Officer" who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations. The name, designation and address of the Principal Officer is required to be communicated to the FIU-IND and also to RBI .

MAFIL has nominated Chief Compliance Officer of the Company as the "Principal Officer" and the corresponding details have been communicated to RBI. MAFIL shall ensure to communicate any change in the name and details of the "Principal Officer" to FIU-IND and RBI whenever it occurs.

8 COMPLIANCE OF KYC POLICY:
In accordance with the Master Directions, the Company shall ensure compliance with KYC Policy through the following:

i. **Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.**
Senior Management for the purpose of the Policy shall be as defined in the policy.

ii. **Allocation of responsibility for effective implementation of policies and procedures**.
MAFIL has allocated Head – KYC with the responsibility of implementation of this policy and procedures.

iii. **Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements.**
MAFIL shall ensure evaluation on annual basis with regards to the compliance functions and other legal and regulatory requirements. The evaluation reports are presented to the Risk Management Committee.

iv. **Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.**
MAFIL's Internal Audit department carries out verification of the compliance with KYC/AML policies and procedures on a quarterly basis and the corresponding Reports are presented to RMC.

v. **Submission of quarterly audit notes and compliance to the Audit Committee.**
MAFIL has put in place a procedure to pace the Quarterly Audit reports of Internal Auditors to the Audit Committee of the Board.

As part of the Regulatory requirement, MAFIL ensures that decision-making functions of determining compliance with KYC norms are carried out by Internal staff only and not outsourced.

9 KEY ELEMENTS OF THE POLICY

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

This policy covers the following key elements:

a. Customer Acceptance Policy (CAP)
b. Risk management
c. Customer Identification Procedures (CIP)
d. Monitoring of Transactions (including Reporting STR, CTR & CCR) & Ongoing Monitoring

9.1 CUSTOMER ACCEPTANCE POLICY (CAP)

MAFIL as part of its various business activities requires to enroll or to on board the customers wanting to carry out their financial services related transactions. Such transactions range from borrowing related regular transactions to one-off transactions. Such relationships will be either account-based relationship or one-off transaction related relationship where the customer may or may not come back in future. Broadly most of the customer relationship MAFIL has with its customers are for its loan products vended out from its various verticals and very few relationships are transaction based. Details in brief are as under:

Loan Product	Type of relationship
All Loan products extended from various business verticals such as Gold Loan, Auto loan etc	Account based relationship with subsequent transitions during the tenor of the loan arrangement
MTSS related payment of inward remittances from abroad and selling and buying of foreign bank notes (Foreign Exchange) under Money changing activities	Transaction based one off relationship which may or may not repeat in future
Sale of third-party products such as MTSS and domestic money transfer	Transaction based relationship which may or may not occur again

In terms of RBI guidelines, the CAP is one of the four parameters which broadly define the KYC/AML/ Countering the Financing of Terrorism (CFT) guidelines. The CAP has been framed for ensuring compliance with all applicable regulatory guidelines while establishing customer relationship and maintaining the related accounts as per profiles of the customers, the Company shall ensure that: -

a) No account shall be opened in anonymous/ fictitious/ benami/ shell company name(s)

b) No account shall be opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. MAFIL shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

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

d) All the mandatory information that shall be sought for KYC purpose at the time of opening an account and during periodic updation shall be specified.

e) Any additional information, where such information requirement has not been specified in this Policy shall be obtained with the explicit consent of the customer at the time of opening of the account or after opening the account.

f) MAFIL shall apply the CDD procedure at the UCIC level. Accordingly, if an existing KYC compliant customer of the Company desires to open another account or avail any other product or service from the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

g) MAFIL shall apply CDD procedure to be followed for all individuals including all joint account holders while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder of an Individual or related to any legal entity ("LE").

h) MAFIL shall scrutinize and satisfy itself of circumstances in which a customer is permitted to act on behalf of another person/entity, by way of acceptable documentation such as power of attorney etc.

i) The Company shall ensure name screening of the prospective customer. Before opening any account, MAFIL shall ensure that the identity of the prospective customer does not match with any person having any account in the name of individuals/ entities appearing in the lists of individuals and entities, suspected of having terrorist's links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). MAFIL shall have appropriate arrangement.

j) Wherever Permanent Account Number (PAN) is obtained from a customer, MAFIL shall verify the same from the verification facility of the issuing authority

k) Where a required document's equivalent e-document is obtained from the customer, MAFIL shall verify the digital signature as per the provisions of the Information Technology Act, 2000.

l) Where Goods and Services Tax (GST) details are required and submitted, MAFIL shall verity the GST number from the search/verification facility of the issuing authority.

m) The Ultimate Beneficial Owner (UBO) shall be identified/verified necessarily while opening/ maintaining accounts having constitution as Partnership, Limited Companies, Trust etc. as detailed in the CDD para of this policy

n) Wherever accounts are opened and be operated by mandate holder or accounts are opened by intermediaries in fiduciary capacities, MAFIL shall ensure that the circumstances in which the said mandate holder or intermediary is permitted to act on behalf of another person/ entity are clearly spelt out, in conformity with the established law and practice of banking. (SOP)

o) If any Customer is found to be a Politically Exposed Person (PEP) as per knowledge of MAFIL, the account of such person will be approved after appropriate escalation.

p) MAFIL shall carry out Re-KYC exercise whenever due as per the risk profile/ category of the customers and fresh set of KYC documents, latest Photograph & need based financials shall be obtained after appropriate due diligence as detailed in the CDD section.

q) No transaction or account-based relationship is undertaken without following the CDD procedures.

r) All the information collected from the customer for the purpose of opening of account and thereafter shall be treated as confidential details and thereof are not to be divulged for cross selling or other purposes without specific consent from the customer. MAFIL shall ensure that the information sought from the customers are relevant to the perceived risk, are not intrusive and are in conformity with the RBI/other regulatory guidelines issued in this regard.

MAFIL shall ensure that the Customer Acceptance Policy (CAP) guidelines and procedures shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged including the Persons with Disability(PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

Whenever in the process of applying the CAP, any staff member has any suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, the staff member shall not pursue the CDD process, and instead file an STR with FIU-IND.

9.2 RISK MANAGEMENT

The Company shall have a Risk-Based Approach (RBA) which includes the following:

a) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.

b) Risk categorization 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, 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, wire transfers, forex transactions, etc.

c) 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.

d) Differential due diligence and monitoring standards shall be applied based on the risk categorization, additional due diligence will apply on High-Risk category.

e) Risk grading shall be made only in respect of Account based relationships and nor for transaction-based relationships. In case any of the transaction-based relationship gets converted to Account based relationships, corresponding AML/KYC risk grading shall be carried out.

At present MAFIL has used a score-based risk categorization model for categorization of customers into low, medium and High-risk categories. The model is being updated from time to time, in place of incident and value-based risk rating model. The process is executed in two layers with the core categorization conducted on a quarterly basis across all active customers and products, daily categorization is also executed for daily onboarded customers. The specific parameters are detailed in the risk categorization SOP.

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 disclosing ("tipping off") the customer.

MAFIL shall ensure that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive as directed in the Master Directions.

MAFIL in the process of Risk categorization, shall take into account FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc

9.3 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

MAFIL shall undertake identification of customers in the following cases:

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

b. Carrying out any international money transfer operations for a person who does not have an account with MAFIL.

c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained, MAFIL shall consider reporting the same in suspicious transactions to FIU.

d. 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.

e. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

f. When the staff engaging with the customer has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

g. MAFIL shall ensure that introduction is not to be sought while opening accounts.

h. In respect of walk-in customers wanting to carry out one off transaction for receiving any inward remittances from abroad under MTSS scheme as agents or sub agents to principal remitters for buying or selling foreign bank notes being an FFMC, the Company shall obtain ID of the recipient as prescribed in the concerned RBI circular in place.

Dependence of Third-Party Agents

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, MAFIL, may rely on customer due diligence done by a third party, subject to the following conditions:

a. Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
b. Adequate steps shall be taken by the Company to satisfy itself 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.
c. MAFIL shall ensure that 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.
d. The third party shall not be based in a country or jurisdiction assessed as high risk.
e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company
f. 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

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

MAFIL 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:

a. 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.

b. Live location of the Customer (Geotagging) shall be captured to ensure that Customer is physically present in India.

c. The official shall ensure that photograph of the Customer in the Aadhaar/PAN details matches with the Customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the Customer.

d. 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.

e. 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.

f. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

g. 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. MAFIL shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. The liveness check shall not result in exclusion of person with special needs.

h. To ensure security, robustness and end to end encryption, MAFIL shall carry out software and security audit and validation of the V-CIP application before rolling it out.

i. The audio-visual interaction shall be triggered from the domain of MAFIL 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.

j. The video recording shall be stored in a safe and secure manner and bears the date and time stamp.

k. It shall be ensured that the Aadhaar number is redacted or blacked-out.

v- CIP Infrastructure

i) The RE should have complied with the RBI guidelines on minimum baseline cybersecurity 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 RE 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 RE only and all the data including video recording is transferred to the RE'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 RE.

ii) The RE 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.

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

iv) 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.

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

vi) 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.

vii) 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.

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

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.

9.4. CUSTOMER DUE DILIGENCE PROCEDURE (CDD) IN CASE OF INDIVIDUALS

For undertaking CDD, MAFIL shall obtain the required from an individual while establishing an account-based relationship or while dealing with individual who is a beneficial owner, authorized 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. The process for obtaining PAN or Form 60 incase of existing customers and temporary cessation of operations in account till the PAN or Form 60 or equivalent e documents thereof is submitted by the customer is detailed in the KYC SOP.

The following documents are required to be obtained from an individual:

a. A certified copy of Officially Valid Documents (OVD), as given in Annexure I to this policy.
b. One recent photograph (For the gold loan segment, customer's photo to be captured and be kept in the ERP).
c. Permanent Account Number (PAN) or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
d. Such other documents pertaining to the nature of business or financial status specified in this Policy.

9.4.1. OFFLINE VERIFICATION THROUGH PROOF OF POSSESSION OF AADHAAR NUMBER:

MAFIL 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 inthe manner prescribed in the Aadhaar Regulations.

The proof of possession of Aadhaar number where offline verification cannot be carriedout 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 recordsfrom 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.

9.4.2. ACCOUNTS OPENED USING AADHAAR OTP BASED E-KYC, IN NON-FACE-TO FACE MODE

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

9.4.3. VERIFICATION THROUGH DIGITAL KYC:

MAFIL 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. Guidelines on digital KYC process is provided in Annexure V of this policy.

9.4.4. 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, MAFIL 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.

9.5. 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:

i. 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.

ii. 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.

9.6.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 of this policy.

10 SIMPLIFIED PROCEDURES FOR SMALL VALUE LOANS:

In case a person who desires to open an account is not able to produce identity documents as mentioned in Annexure I (i.e., any of OVDs and PAN/ Form 60), Proof of Identity alone will be sufficient provided that the Customer gives full and complete address in the loan application form and his telephone number is confirmed by the branches to be correct. Interim / Temporary KYC documents such as Labour card, Civil ID card, Credit Card, Employer Company ID card, LIC card, State ID card, Bank Passbook, etc. may be accepted subject to the following conditions:

a. The Customer shall provide his self-attested photograph.
b. Branch Head/ Designated Officer of MAFIL shall certify under his/her signature that the Customer has affixed his signature or thumb impression in his presence.
c. The account shall remain operational initially for 12 months, within which the Customer must furnish his identity documents for conducting CDD as mentioned in para 6.3. Customer shall be suitably informed at the time of starting the relationship.
d. Maximum outstanding shall not exceed Rs 0.50 Lakh in all their accounts taken together at any point of time and the total credit in all the accounts taken together shall not exceed Rs. 1.00 lakh in a year.
e. The Customer shall be made aware that no further transaction will be permitted until full KYC procedure is completed in case of condition no. d. as mentioned above is breached.
f. Regularization of Interim/Temporary KYC: In-order to avoid any inconvenience to the Customers MAFIL shall notify the Customer when the balance reaches rupees forty thousand (Rs. 40,000/-) or the total credit in a year reaches rupees eighty thousand(Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted and that otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds Rs.0.50 lakh at any point of time or the total credit in the accounts in year exceeds Rs 1.00 Lakh.
g. Permanent and communication address of the customer is collected through the application form submitted.
h. The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per Section 16 or Section 18 of KYC Master Direction.

KYC verification once done by one branch shall be valid for transfer of account to any other branch, provided full KYC verification has already been done and the same is not due for periodic updating.

11 SELLING THIRD PARTY PRODUCTS:

While selling third party products, MAFIL shall comply with the following directions:

a. Identity and address of the walk-in Customers shall be verified for transactions above Rs. 0.50 lakh, whether conducted as a single transaction or several transactions that appear to be connected.
b. Transaction details of sale of third-party products and related records shall be maintained as specified under this Policy.
c. AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with Customers including walk-in Customers shall be made available.
d. Transactions involving Rs 0.50 lakh and above shall be undertaken only by:
   - Debit to Customer's account or against cheque, transfer from banks / debit cards / credit card etc.
   - Obtaining and verifying PAN (regular Customer as well as walk in Customer).

Note: Direction no. d shall also apply to sale of MAFIL's own products, sale and reloading of prepaid / travel cards and any other products for Rs 0.50 lakh and above.

12 ISSUANCE OF PREPAID PAYMENT INSTRUMENTS (PPI)

With regard to PPI, MAFIL shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

13 ONGOING DUE DILIGENCE

a. MAFIL 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.

b. Without prejudice to the generality of factors that call for close monitoring, the following types of transactions are monitored closely: -
   i) 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.
   ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.
   iii) High account turnover inconsistent with the size of the balance maintained.
   iv) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

c. The extent of monitoring shall be aligned with the risk category of the Customer. Customer classified as High risk will be subject to more intensified monitoring.
   i) 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.
   ii) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

14 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 procedure laid down below. Also, incase the validity of the document expires, the Customer shall not be able to make any further transactions until the revised document is submitted to the Company.

Not with standing the provisions given above, in respect of an individual customer who is categorized as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later.

The Company shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

a. FOR INDIVIDUAL CUSTOMERS

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

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

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 MAFIL, digital channels (such as mobile application of MAFIL), letter from an official authorized by the Legal Entity in this regard, board resolution etc. Further, MAFIL 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.

ii. **Change in KYC information:** In case of change in KYC information, MAFIL 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, MAFIL shall also ensure that,

i. 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 MAFIL are not as per the existing CDD standards. Further, in case the validity of the CDD documents available with MAFIL has expired at the time of periodic updation of KYC, MAFIL shall undertake the KYC process equivalent to that applicable for on-boarding a new Customer.
ii. Customer's PAN details, if available with the MAFIL, is verified from the database of the

issuing authority at the time of periodic updation of KYC.

iii. 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 updation / periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/ periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, MAFIL may consider making available the facility of updation / periodic updation of KYC at any of its branches.

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

MAFIL 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; MAFIL 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 MAFIL's end.

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

Due Notices for Periodic Updation of KYC

The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, MAFIL shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, MAFIL shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail. The intervals for intimation of periodic updation shall be as specified in the SOP".

15 EXISTING CUSTOMERS – MANDATORY REQUIREMENT TO SUBMIT PAN

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

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

The Company shall not put any restriction on operations in the accounts where an inf has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

16. ENHANCED DUE DILIGENCE

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

a. 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 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;

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

c. 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.

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

3. 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.” MAFIL 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.

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

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

a. withdrawal or deposit in cash, exceeding such amount;
b. transaction in foreign exchange, exceeding such amount;
c. transaction in any high value imports or remittances;
d. 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.

16.1 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, MAFIL 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.

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 MAFIL 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.

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

The following customers have been identified as the PEP for the purpose of the Policy:

1. Celebrities/Actors/Close Relative/Associates of such person
2. Magistrate/Judge/Close Relative/Associates of such person
3. MD/CEO/Chairman of Established Organization/Close Relative/Associates of such person
4. MD/CEO/Chairman of Public Corporation/Close Relative/Associates of such person
5. Religious Leaders/Close Relative/Associates of such person
6. Senior Executive in Press and Media/Close Relative/Associates of such person
7. Senior Officials of Govt Organization/Close Relative/Associates of such person
8. Senior Politician/MP/MLA/Minister/Close Relative/Associates of such person
9. Senior Ranked Police/Military Officer/Close Relative/Associates of such person

16.2 ACCOUNTS OF NON-FACE-TO-FACE CUSTOMERS: These Customers are those who opened accounts without visiting the branches / offices of MAFIL or meeting its officials. MAFIL shall ensure that first payment from these accounts shall be affected through the Customers' KYC- Complied account with another Regulated Entity.

16.3 Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

Non-face-to-face onboarding facilitates the Company 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 Section 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 the Company for non face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

a) The process of V-CIP shall be provided as the first option to the customer for remote onboarding as it shall be treated on par with face-to-face CIP.
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. Also, the Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
c) Apart from obtaining the current address proof, the Company 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.
d) MAFIL 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

16.4 CLIENT ACCOUNTS OPENED BY PROFESSIONAL INTERMEDIARIES:

MAFIL 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. MAFIL 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. MAFIL shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to MAFIL.
d. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of MAFIL, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of MAFIL, the MAFIL shall look for the beneficial owners.

e. MAFIL 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.
f. The ultimate responsibility for knowing the Customer lies with MAFIL.

16.5 CLIENTS OF SPECIAL CATEGORY (CSC):

As per the guidelines on AML standards of SEBI, enhanced due diligence is required for Customers belonging to CSC (Eg. non – residents, High net worth clients etc). Appropriate measures shall be exercised by way of independent judgment to ascertain whether new clients engaged through DP services need to be classified as CSC or not. An illustrative list of Special Category Customers identifiable to DP is given in Annexure IV.

16.6 Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex III, subject to Income Tax (FATCA/CRS) Rules. Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex III will be submitted

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

For the cases where reporting under FATCA and CRS is applicable, the Company shall comply with the requirements as specified in the Master Directions dated 06th November, 2024

17.CONFIDENTIALITY OF INFORMATION ABOUT CUSTOMERS

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

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

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

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

18. MAINTENANCE OF RECORDS OF TRANSACTIONS

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

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

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

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

d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules.

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

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

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

Explanation. – For the purpose of this Section, 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. MAFIL 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, MAFIL shall register the details on the DARPAN Portal. MAFIL shall also maintain such registration records for a period of five years after the business relationship between the customer and the MAFIL has ended or the account has been closed, whichever is later.

.

19. GENERAL:

19.1 ADHERENCE TO KYC GUIDELINES BY AGENTS/ BROKERS OR THELIKE

a. 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 MAFIL.
b. MAFIL shall make available all information to RBI to verify the compliance with KYC guidelines. MAFIL shall be responsible for non-customer guidelines by the brokers/agents etc. who are operating on MAFIL's behalf.

19.2 STAFF AND MANAGEMENT RESPONSIBILITIES – OFFENCE OF MONEY LAUNDERING

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

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

MAFIL 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 PML Rules, as amended from time to time. Additionally, MAFIL 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.

MAFIL shall also ensure that during periodic updation of the Customers, the Customers are migrated to the current CDD standard as applicable to MAFIL. 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.

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

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, the Company shall ensure that the same is communicated to the individual/LE as the case may be.

Whenever MAFIL obtains additional or updated information from any customer as per the clause below or Rule 9 (1C) of the PML Rules, MAFIL shall within 7 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. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs MAFIL regarding an update in the KYC record of an existing customer, MAFIL shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by it.

For the purposes of establishing an account-based relationship, updation / periodic updation or for verification of identity submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then MAFIL 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 –

I. There is a change in the information of the customer as existing in the records of CKYCR;
II. The KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
III. The current address of the customer is required to be verified;
IV. The Company 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 client.
V. The validity period of documents downloaded from CKYCR has lapsed.

19.4. TRAINING PROGRAMME

MAFIL shall have adequate screening mechanism as an integral part of personnel recruitment / hiring process and should have an ongoing employee training programs so that 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 can fully understand the rationale behind the KYC policies and implement them consistently. Such training may be a mix of in-house as well as through external agencies, as the case may be.

20. COMPLIANCE WITH POLICY NORMS

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

21. OTHER OPERATING INSTRUCTIONS

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

22. WIRE TRANSFER:-

A. Information requirements for wire transfer for the purpose of the Policy:

i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:
   a. name of the originator
   b. the originator account number where such an account is used to process the transaction
   c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
   d. name of the beneficiary; and
   e. the beneficiary account number where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

ii. In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

iii. Domestic wire transfer, where the originator is an account holder of the ordering Company, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

iv. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering company, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers. In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering company and where the information accompanying the wire transfer can be made available to the beneficiary company and appropriate authorities by other means, it is sufficient for the ordering company to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. Further, the ordering company shall make the information available within three working/business days of receiving the request from the intermediary company, beneficiary company, or from appropriate competent authorities.

v. The Company shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

vi. The wire transfer instructions are not intended to cover the following types of payments:

a) Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to- person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

However, these instructions will not impact the obligation of the Company to comply with applicable reporting requirements under PML Act, 2002, and the PML Rules made thereunder, or any other statutory requirement in force.

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

a. The Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 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.

b. 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.

c. Further, the Company 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.

d. 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 Section 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. The Company shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted. It maybe noted that in terms of Paragraph 1 of the Order, Director, FIU-IND has been designated as the CNO.

e. The Company may refer to the designated list, as amended from time to time, available on the portal of FIU-IND.

f. In case there are reasons to believe beyond doubt that funds or assets held bya customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 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.

g. In case an order to freeze assets under Section 12A is received by the Company from the CNO, the Company shall, without delay, take necessary action to comply with the Order.

h. 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.

i. The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', 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.

j. In addition to the above, the Company 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 Section 51A of the UAPA and Section 12A of the WMD Act.

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

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

All offices shall ensure that in terms of Section 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:

a. 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.

b. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution1988 (2011), which includes names of individuals and entities associated with the Taliban.

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.

Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 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.

2. NON-INDIVIDUALS (Companies, Firms, Trusts etc.)

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

Legal entities (Companies)	Self 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. f) the names of the relevant persons 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: a) Registration certificate. b) Partnership deed. c) PAN of the partnership firm

	d) Documents as specified in para 1 above of the individuals holding attorney /authorization to transact on its behalf. e) 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) shall be carried out PLUS any two of the below mentioned documents, a) Registration certificate including Udyam Registration Certificate (URC) b) Certificate/License issued under Shops & Establishment Act c) GST and Income Tax returns d) GST registration certificate (provisional/ final) e) Utility bills such as electricity, water, telephone bills etc. f) 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. g) 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 MAFIL is satisfied that it is not possible to furnish two such documents, MAFIL may, at its discretion, accept only one of those documents as proof of business/activity. Provided MAFIL 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: a) Certificate of Registration; b) Trust Deed c) Power of Attorney authorizing a person to carry out transactions on behalf of the trust d) Permanent Account Number or Form No.60 of the trust; and e) 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 f) 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 authorized 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: (a) Resolution of the managing body of such association or body of individuals

	(b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals (c) Power of attorney granted to transact on its behalf (d) Documents, as specified in Para 1, of the person holding an attorney to transact on its behalf and (e) Such information as may be required by MAFIL 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 authorized 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 MAFIL to establish the legal existence of such an entity/juridical person.

Annexure II

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 /Fake 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. UNEXPLAINED TRANSFERS:

a) 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 Bonafede 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 TRANSACTION:

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

b) Submission of fake 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 III

CUSTOMERS OF SPECIAL CATEGORY (CSC):

SPECIAL CATEGORY CUSTOMERS IDENTIFIABLE IN DP :-

a. Non-Resident Customers

b. High Net worth Customers,

c. Trust, Charities, NGOs, and organizations receiving donations

d. Companies having close family shareholdings or beneficial ownership

e. Politically exposed persons (PEP) of foreign origin

f. Current / Former Head of State, Current or Former Senior High-profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)

g. Companies offering foreign exchange services.

h. Customers in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. Non face to face Customers.

i. Customers with dubious reputation as per public information available etc. The above-mentioned list is only illustrative and not exclusive

Annexure IV

DIGITAL KYC PROCESS (RBI GUIDELINES)

A. The Company 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 Company.

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 color 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.

l. 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.

k) 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.

l) 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.