MUTHOOT CAPITAL SERVICES LIMITED

CIN: L67120KL1994PLC007726

POLICY GUIDELINES ON 'KNOW YOUR CUSTOMER' NORMS AND ANTI - MONEY LAUNDERING MEASURES

The Policy is approved by the Board on January 30, 2015 and last reviewed on May 19, 2023 , May 23, 2024 and March 24, 2025

Version Control:

Sl. No.	Name of Policy	Version	Board approval date	Remarks
1.	PMLA - KYC Policy	v1.0	30/01/2015	Policy document approved.
2.	PMLA - KYC Policy	v1.1	10/11/2017	Substituted the Clause (5) - Monitoring of Transactions.
3.	PMLA - KYC Policy	v1.2	14/06/2018	Incorporated the applicable provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
4.	PMLA - KYC Policy	v1.3	24/04/2019	Incorporated the Risk Categorization Matrix.
5.	PMLA - KYC Policy	v1.4	29/07/2019	Amended Clause 5 (i) to to validate the customer profiles in the SHERLOCK - AML database.
6.	PMLA - KYC Policy	v1.5	30/01/2021	Incorporated new clause 8 - Sharing KYC information with Central KYC Records Registry (CKYCR).
7.	PMLA - KYC Policy	v1.6	19/05/2023	Incorporated the following: - 1)clause m added under 5. Customer Acceptance Policy (CAP)-RE'S shall advice customer to comply to PML policy. 2)added (v), (vi) on documents required for a company under 7.e Customer Due Diligence (CDD) Procedure 3)added (iv), (v) on documents required for a partnership firm

				under 7.e Customer Due Diligence (CDD) Procedure 4)added (iv),(v) & (vi) on documents required for a trust firm under 7.e Customer Due Diligence (CDD) Procedure
8.	PMLA - KYC Policy	v1.7	23/05/2024	Amended as per the latest regulations
9.	PMLA - KYC Policy	v1.8	24/03/2025	Amended to include Whole Time Director as an alternative to Managing Director

POLICY GUIDELINES ON 'KNOW YOUR CUSTOMER' NORMS AND ANTI-MONEY LAUNDERING MEASURES

1. Introduction:

As per the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Non-Banking Finance Companies (NBFCs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for NBFCs thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers vide Master Direction - Know Your Customer (KYC) Direction, 2016 DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, as amended on April 20, 2018.

Muthoot Capital Services Limited (MCSL or the Company) shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this code to conform to the standards so prescribed. This policy is applicable across all branches / business segments of the company and is to be read in conjunction with related operational guidelines issued from time to time.

The contents of the Policy shall always be read in tandem/auto-corrected with the changes/modifications which shall be advised by RBI from time to time.

MCSL endeavors to frame a proper policy framework on 'Know Your Customer' (KYC) and Anti- Money Laundering measures. The Company is committed for transparency and fairness in dealing with all stakeholders and in ensuring adherence to all laws and regulations.

The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof for cross selling or any other purposes. The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his/her consent and after effective rendering of services. The Company shall also communicate its KYC norms to its customers. The Company shall ensure that the implementation of the KYC norms is the responsibility of the entire organization.

The Board of Directors and the Management team of the Company are responsible for implementing the KYC norms hereinafter detailed and also to ensure that its operations reflect its initiatives to prevent money laundering activities.

2. 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

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

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

(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 percent of capital or profits of the partnership or who exercises control through other means.

"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 has/have ownership of/entitlement to more than 15 percent 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 percent 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). Customer'

A 'Customer' shall be defined as:

a. A person or entity that maintains and/or has a business relationship with the Company;
b. One on whose behalf such relationship is maintained (i.e. the beneficial owner)
c. Business intermediaries as permitted under the law, and;
d. Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say, a wire transfer or issue of a high value demand draft as a single transaction.

(iii). Customer Due Diligence (CDD)

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

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.

(iv)" Officially Valid Document" (OVD) means the passport, the driving licence, 16proof 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:-

utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); property or Municipal tax receipt; pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

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: 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.

(iv). "Politically Exposed Persons" (PEPs).

PEPs are individuals who are or have been entrusted with prominent public functions **by a foreign country**, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

(v). Suspicious transaction

"Suspicious transaction" means a "transaction" as defined above, 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, 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: Transactions involving 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.

3. Objective:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The Policy explains the following four key elements:

a. Customer Acceptance Policy;
b. Risk Management;
c. Customer Identification Procedures; and
d. Monitoring of Transactions.

4. Appointment of Designated Director and Principal Officer

The Managing Director or Whole Time Director shall act as the Designated Director who shall ensure the overall compliance with the obligations imposed under the Prevention of Money Laundering Act, 2002 and Rules made thereunder.

The Chief Operating Officer/ Chief Executive Officer of the Company is the Principal Officer located at the registered/ corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information

as required under the law/regulations. He shall maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

5. Compliance of KYC Policy

The Company shall ensure compliance with this Policy through:

a. Senior Management including Managing Director or Whole Time Director, Chief Operating Officer, Chief Executive Officer, wherever they are appointed, shall ensure the effective implementation of this Policy;
b. Concurrent or Internal Audit system shall verify the compliance with KYC/AML policies and procedures.
c. Submission of quarterly audit notes and compliance by the Concurrent or Internal Audit to the Audit Committee of the Board.

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

6. Customer Acceptance Policy (CAP)

As part of the Customer Acceptance Policy, the Company shall ensure that:

a. No account is opened in anonymous or fictitious/ benami name(s);
b. No account is opened where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The CDD Procedure shall be followed for all the joint account holders, while opening a joint account. It shall be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
c. The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category;
d. Accept customers after verifying their identity as laid down in customer identification procedures;
e. While carrying out CDD, the Company shall ensure that the procedure adopted shall not result in denial of services to the genuine customers;
f. For the purpose of risk categorization of customer, Company shall obtain the relevant information from the customer at the time of account opening. Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and

financial status etc. to enable categorization of customers into low, medium and high risk; customers requiring very high level of monitoring, if considered necessary, be categorized even higher. The Customer Risk Categorization matrix to be followed by the Company is attached herewith as **Annexure I**.

g. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money-Laundering Act, 2002 and guidelines issued by Reserve Bank from time to time;

h. Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice as there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity;

i. Necessary checks before opening a new account to ensure that suitable system is put in place to confirm that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India;

j. The Company shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/ financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the company. However, while preparing customer profile the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes;

k. Adoption of Customer Acceptance Policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.

l. As advised by RBI under Circular No. DNBS(PD)CC.No.193/03.10.42/2010-11, the Company shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

m. MCSL shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of

establishment of business relationship / account-based relationship and thereafter, as necessary, customers shall submit to the MCSL 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 MCSL end.

7. Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. The Company may also rely on customer due diligence done by a third party subject to the conditions specified in the KYC Master Direction. Being satisfied means that the Company must be able to satisfy the competent authorities that CDD was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).

Customer Identification Procedure is to be carried out at different stages i.e.

- While establishing a business relationship (or)
- Carrying out a financial transaction (or)
- Where the Company has a doubt about the authenticity/veracity (or) inadequacy of the previously obtained customer identification data if any.

When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

8. Customer Due Diligence (CDD) Procedure

For undertaking CDD, the Company shall obtain the following information:

a) i) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number; the Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time;

ii) Where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an Officially

Valid Document (OVD) (as mentioned in **Annexure II**) containing details of identity and address and one recent photograph shall be obtained.

In case the above customer fails to submit the Aadhaar number or Permanent Account Number/Form No. 60 within six months from the commencement of the account based relationship, the said account shall cease to be operational till the time the Aadhaar number and Permanent Account Number/Form No. 60 is submitted by the customer.

iii) An explicit consent from the customer may be obtained to subject himself/herself to e-KYC verification (biometric or OTP). While seeking explicit consent of the customer, the consent provisions as specified in Section 5 and 6 of the Aadhaar (Authentication) Regulations, 2016, shall be observed.

iv) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and any rules issues thereunder and take a live photo as specified under Annexure III v) any OVD or proof of possession of Aadhaar number above where offline verification cannot be carried out, MCSL shall carry out verification through digital KYC as specified under Annexure III

v) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR.

Provided that for a period not beyond such date as may be notified by the Government for a class of the Company, instead of carrying out digital KYC, the Company pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, The Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception,

customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review.

b) From an individual who is not eligible to be enrolled for an Aadhaar number, or who is not a resident, the following shall be obtained:

i. PAN or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time;
ii. one recent photograph; and
iii. A certified copy of an OVD containing details of identity and address.

In such cases, a declaration to the effect of individual not being eligible for enrolment of Aadhaar may also be obtained by the Company.

Provided that, in case the OVD furnished by the customer does not contain updated address, the Company may require the additional documents as mentioned in **Annexure II** for the limited purpose of proof of address. However, the Company shall require the customer to submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

At the time of receipt of Aadhaar number, the Company shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication subject to the following:

i. Yes/No authentication shall not be carried out while establishing an account based relationship.
ii. In case of existing accounts where Yes/No authentication is carried out, the Company shall carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out Yes/No authentication.
iii. Yes/No authentication in respect of beneficial owners of a legal entity shall suffice in respect of existing accounts or while establishing an account based relationship.

The Company shall ensure that the information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

c) In case a person who desires to establish a business relationship with the Company is not able to produce identification information as mentioned above, the Company

may at its discretion establish a business relationship subject to the following conditions:

i) The Company shall obtain a self-attested photograph from the customer;
ii) The designated officer of the Company shall certify under his signature that the person opening the account has affixed his/her signature or thumb impression in his presence;
iii) The account shall remain operational initially for a period of twelve months, within which the customer has to furnish identification information as mentioned under Clause 8 (a) or (b) of this Policy as applicable;
iv) The identification process as per Clause 8 (a) or (b) of this Policy is to be completed for all the existing accounts opened on the basis of introduction earlier, within a period of six months;
v) The balances in all their accounts taken together shall not exceed ₹ 50,000/- at any point of time;
vi) The total credit in all the accounts taken together shall not exceed ₹ 1,00,000/- in a year;
vii) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (v) and (vi) above are breached by him;
viii) OVDs of those with ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company
ix) The customer shall be notified when the balance reaches ₹ 40,000/- or the total credit in a year reaches ₹ 80,000/- that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (v) and (vi) above.

Note: Obtaining a certified copy by the Company shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the Company.

d) For customers that are Sole Proprietary firms, the Company shall obtain the following documents as OVDs:

(i) Identification information as mentioned under Clause 8 (a) or (b) of this Policy/OVDs in respect of the individual (proprietor);

(ii) Any two of the following documents as a proof of business/ activity in the name of the proprietary firm:

- Registration certificate;
- Certificate/license issued by the municipal authorities under Shop and Establishment Act;
- Sales and income tax returns;
- CST/VAT/ GST certificate (provisional/final);
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities;
- IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;
- 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;
- Utility bills such as electricity, water, and landline telephone bills.

Where the Company is satisfied that it is not possible to furnish two such documents, the Company may at their discretion, accept only one of those documents as proof of business/activity and in such cases, the Company 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.

e) For customers that are legal entities, the Company shall obtain the certified true copies of the following documents:

❖ <u>Company</u>:

(i) Certificate of incorporation;
(ii) Memorandum and Articles of Association;
(iii) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
(iv) Identification information as mentioned under Clause 8 (a) or (b) of this Policy in respect of managers, officers or employees holding an attorney to transact on its behalf.
(v) The names of the relevant persons holding senior management position
(vi) The registered office and the principal place of its business, if it is different.
(vii) Certified True copy of latest Shareholding pattern

(viii) OVDs of those with ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company

- Partnership Firm:

(i) Registration certificate.
(ii) Partnership deed.
(iii) Identification information as mentioned under Clause 8 (a) or (b) of this Policy in respect of the person holding an attorney to transact on its behalf.
(iv) The names of all the partners
(v) The address of the registered office, and the principal place of its business, if it is different.
(vi) Identification information as mentioned under Clause 8 (a) or (b) of this Policy in respect of the person holding more than 10 percent of capital or profits of the partnership or who exercises control through other means.
(vii) OVDs of those who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means

- Trust:

(i) Registration certificate.
(ii) Trust deed.
(iii) Identification information as mentioned under Clause 8 (a) or (b) of this Policy in respect of the person holding an attorney to transact on its behalf.
(iv) The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
(v) The address of the registered office of the trust
(vi) The list of trustees and documents, as specified for those discharging the role as trustee and authorized to transact on behalf of the trust
(vii) OVDs of author of the trust, the trustee, the beneficiaries with 10 percent 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

- Unincorporated Association or a Body of Individuals:

(i) Resolution of the managing body of such association or body of individuals;
(ii) Power of attorney granted to transact on its behalf;

(iii) Identification information as mentioned under Clause 8 (a) or (b) of this Policy in respect of the person holding an attorney to transact on its behalf; and

(iv) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

(e) OVDs of who, whether acting alone or together, or through one or more juridical has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

- Juridical persons such as Government or its Departments, societies, universities and local bodies like village panchayats:

(i) Document showing name of the person authorised to act on behalf of the entity;

(ii) Aadhaar/PAN/OVDs for proof of identity and address in respect of the person holding an attorney to transact on its behalf; and

(iii) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Provided that in case of a trust, the Company shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions specified below.

a. 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.
b. When the Company 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.

The Company shall take necessary steps to understand the ownership and control structure of the customer and determine who the natural persons are and who ultimately control the legal person. The Company shall frame its own internal guidelines based on their experience of dealing with such persons/entities, normal lenders prudence and the legal requirements as per established practices. The Company shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

The authorised officer of the Company shall verify the copy of such OVD produced by the customers with the originals and shall record the same by affixing the 'Original Seen and Verified' seal with his signature on the copy of the documents to ensure the authenticity.

The documents requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds/wealth. The extent of monitoring shall be aligned with the risk category of the customer.

The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. 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 by way of PAN verification, Aadhaar authentication, obtaining certified true copy of OVDs, etc.

No deviations or exemptions shall normally be permitted in the documents specified for account opening. In case of any extreme cases of exceptions, concurrence of Managing Director or Whole Time Director shall be obtained duly recording the reasons for the same.

The Company shall follow the indicative guidelines on the customer identification requirements as given in **Annexure IV**.

9. Digital KYC

"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the branch. The detailed process of digital KYC is explained in **Annexure III**

10. Video based Customer Identification Process (V-CIP)

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

Accounts, both deposit and borrower, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out, If Aadhaar details are used, the process shall be followed in its entirety including fresh Aadhaar OTP authentication

MCSL may undertake V-CIP to carry out:

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

   Provided that in case of CDD of a proprietorship firm, MCSL shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm apart from undertaking CDD of the proprietor.

ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.

iii. Updation/Periodic updation of KYC for eligible customers

MCSL opting to undertake V-CIP, shall adhere to the following minimum standards

a. **V-CIP Infrastructure**

(1). MCSL should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for NBFCs, 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 MCSL 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 MCSL only and all the data

including video recording is transferred to the MCSL'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 MCSL.

(2). MCSL 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.

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

(4). 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.

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

(6). 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-security event under extant regulatory guidelines.

(7). 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 empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(8). The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and 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.

b. V-CIP Procedure

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

(2). Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.

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

(4). Any prompting, observed at end of customer shall lead to rejection of the account opening process.

(5). The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

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

(a) OTP based Aadhaar e-KYC authentication

(b) Offline Verification of Aadhaar for identification

(c) KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer

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

Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16 where the authentication of Aadhaar number is not required.

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 working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Bank shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Bank shall ensure that no incremental risk is added due to this.

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

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

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

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

(11). All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

(12). All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the MCSL.

c. V-CIP Records and Data Management.

The entire data and recordings of V-CIP shall be stored in a system / systems located in India. MCSL shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

- The activity log along with the credentials of the official performing the V-CIP shall be preserved.

11. Updation / Periodic Updation of KYC

MCSL shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation.

12. Sharing KYC information with Central KYC Records Registry (CKYCR)

a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
b) In terms of provision of Rule 9(1A) of 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.
c) The Company shall adhere to the Operational Guidelines for uploading the KYC data released by CERSAI from time to time.
d) The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be.
e) **Know Your Client (KYC) Identifier** is a unique number or code assigned to a customer by the Central KYC Records Registry. Once KYC Identifier is generated by CKYCR, the Company shall communicate the same to the Individual/LE customer as the case may be.
f) The customer for the purpose of creating an account with the Company **can share his/her KYC Identifier along with an explicit consent to download records from CKYCR,** whereupon the Company shall retrieve the KYC records online from CKYCR using the KYC Identifier and complete the KYC formalities**.**
g) In this way, the customer need not submit the same KYC records or information or any other additional identification documents or details to the Company unless:
    (i) there is a change in the information of the customer as existing in the CKYCR or

(ii) the current address is required to be verified or

(iii) the Company considers it necessary to verify identity/address of customer or perform enhanced due diligence or build appropriate risk profile of client.

13. Monitoring of Transactions

The Company is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the address: Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi - 110021.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. MCSL shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

Directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

The Company shall adhere to the following:

a. The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month;
b. The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction;
c. The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
d. Utmost confidentiality should be maintained in filing of CTR and STR with FIU-IND.
e. It should be ensured that the reports for all the branches are filed in one mode i.e. electronic or manual;
f. A summary of cash transaction report as a whole may be compiled by the Principal Officer in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted both for manual and electronic reporting.

The Company may not put any restrictions on operations in the accounts where an STR has been made. However, it should be ensured that there is no tipping off to the customer at any level. It is likely that in some cases, transactions are abandoned/ aborted by

customers on being asked to give some details or to provide documents. The Company should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

The Company should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in the Schedule of PMLA, 2002.

In terms of instructions contained in the guidelines on 'Know Your Customer Norms' and 'Anti-Money Laundering Measures' of our circular dated February 21, 2005, MCSL is required to prepare a profile for each customer based on risk categorization. Further, vide paragraph 4 of our circular DNBS (PD). CC 68 /03.10.042/2005-06 dated April 5, 2006, the need for periodical review of risk categorization has been emphasized. As a part of transaction monitoring mechanism, it is required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transactions.

It is required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at Principal Officer level should be properly recorded.

14. Maintenance of records of transactions

The Company shall introduce a system of maintaining proper record of transactions as mentioned below:

a. all cash transactions of the value of more than ₹ 10 lakhs or its equivalent in foreign currency;
b. all series of cash transactions integrally connected to each other which have been valued below ₹ 10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds ₹ 10 lakhs;
c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

d. all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

15. Preservation of records

The Company shall maintain the following information in respect of transactions referred to in Rule 3:

a. the nature of the transactions;
b. the amount of the transaction and the currency in which it was denominated;
c. the date on which the transaction was conducted; and
d. the parties to the transaction.

The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

Further, the Company shall maintain for at least ten years from the date of cessation of transaction between the company and the client, all necessary records of transactions, both domestic or international, which shall permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The Company shall ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data shall be made available to the competent authorities upon request.

16. Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, the Company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

The Company shall adopt the format prescribed; follow timelines, guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. The Company shall initiate urgent steps to ensure electronic filing of cash transaction report (CTR). The Company shall not put any restrictions on operations in the accounts where an STR has been made. However, it shall be ensured that there is no tipping off to the customer at any level.

For determining integrally connected cash transactions, NBFCs shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds ₹ 10 lakhs during the month.

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The Company shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. The company shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction. The Company shall make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the Company shall consider the indicative list of suspicious activities contained in **Annexure VI**.

17. Risk Management

The Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles of their existing and new customers and apply various anti money laundering measures keeping in view the risks involved

in a transaction, account or business relationship. The Company's internal audit and compliance functions shall have an important role in evaluating and ensuring adherence to the KYC policies and procedures.

As a general rule, the compliance function shall provide independent evaluation of the Companies own policies and procedures including legal and regulatory requirements. The Company shall ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures.

Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals.

The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

18. Customer Education

Implementation of KYC procedures requires the Company to demand certain information from customers which shall be of personal nature or which have hitherto never been called for. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company shall prepare specific literature/pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staffs shall be specially trained to handle such situations while dealing with customers.

19. Combating financing of terrorism

a) In terms of PMLA Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit - India (FIU-IND) on priority.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council

Resolutions (UNSCRs), is circulated by Reserve Bank, the Company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities shall be accessed in the United Nations website at https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list. The Company shall before opening any new account, ensure that the name/s of the proposed customer does not appear in the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels.

Adequate screening mechanism shall be put in place by the company as an integral part of recruitment/hiring process of personnel.

The Company shall take into account risks arising from the deficiencies in AML/CFT regime of countries of Iran, Angola, Democratic People's Republic of Korea (DPRK), Ecuador, Ethiopia, Pakistan, Turkmenistan and Sao Tome and Principe and list of countries circulated by RBI from time to time.

20. Money Laundering and Terrorist Financing Risk Assessment by the Company:

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

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

(b) The risk assessment by the MCSL shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the MCSL. Further, the periodicity of risk assessment exercise shall be determined by the Board **or any committee of the Board of the Company to which power in this regard has been delegated**, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent uthorities and self-regulating bodies.

(d) MCSL shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. MCSL shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, MCSL shall monitor the implementation of the controls and enhance them if necessary.

Annexure - I

CUSTOMER RISK CATEGORIZATION MATRIX

Customer Risk in the current context refers to "money laundering and terrorist funding risk" associated with a particular customer from the NBFC's perspective. This risk is based on risk perception associated with customer profile and level of risk associated with the product offered

For categorizing a customer as low risk, medium risk, and high risk, the parameters considered are: - customer's identity, - social/financial status, - nature of business activity, etc. No financial sector business is immune from the activities of criminal elements. However, given the very nature of the process and transactions of the NBFCs are only through bank channels, it is minimal in nature. The level of money laundering risk that NBFC is exposed to by a customer relationship depends on:

1. Type of customer and nature of business
2. Type of product/service availed by customer

RETAILS & CORPORATE LOANS RISK CATEGORIZATION

LOW RISK CUSTOMERS (LEVEL 1 CUSTOMERS):

Low Risk Individuals and entities whose identities and sources of income/wealth can be easily identified may be categorized as Low Risk Customers.

Customers availing an asset-based or consumer loan of less than ₹ 5 lakhs will be classified as low risk customers.

Corporate entities not falling under high risk and secured loan amount upto INR 5 crs for retail lending having good corporate governance and sound business practices, transaction through banking channels, a robust Board and reputed shareholders and

profitable track record for a period of at least 2 years may also be categorized as Low Risk Customers.

Category of low risk customers may also include, but may not be limited to, salaried employees with well-defined salary structure from a Corporate entity, people working with Government Companies/Departments, Regulatory/Statutory Bodies, public sector units, reputed public limited companies and Multi-National Companies, etc., dependent members of the family (housewives/students), people belonging to lower economic strata of the society whose accounts show small balances and low turnover, etc. For this category, KYC requirement would be proper identification proof and verification of proof of address.

MEDIUM RISK CUSTOMERS (LEVEL 2 CUSTOMERS):

Customers who are likely to pose a higher than average risk to the Company should be categorized as Medium Risk Customers. Customers particularly whose sources of fund are not clear, and transaction exceeds the disclosed source of fund would fall in this category. Customers availing an asset-based or consumer loan of more than ₹ 5 lakhs may be categorized as Medium Risk Customers.

Corporate entities not falling under high risk and availing secured loans > 5crs for retail lending having good corporate governance and sound business practices, transaction through banking channels, a robust Board and reputed shareholders and profitable track record for a period of at least 2 years may also be categorized as Medium Risk Customers.

Category of medium risk customers may include, but may not be limited to, salaried employees with unstructured income, people working with partnership firms, proprietary concerns, etc., self-employed personnel other than High Net Worth Individuals, self-employed customers with sound business and profitable track record for a reasonable period, etc. For this category, KYC requirement would be proper identification and verification of proof of address

HIGH RISK CUSTOMERS (LEVEL 3 CUSTOMERS):

High Risk Customers are those who are engaged in certain business or profession where money laundering possibilities are high. For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, sources of funds, besides proper identification.

For categorisation, Customers, in the informal segment, availing secured /unsecured loans (other than retail lending) should be categorised as High-Risk Customers if they belong to the below categories :

1. Sole Proprietorship & Partnership in corporate business segment
2. Trusts, Charities, NGOs, and organizations receiving substantial amount of its donations from non-Banking/ unidentifiable channels.
3. Companies having close family shareholding or beneficial ownership but lack proper Corporate Governance structure
4. Firms having sleeping partners
5. Non-resident customers
6. High Net Worth Individuals
7. Accounts under Foreign Contribution Regulation Act
8. Accounts of non-face to face customers
9. Politically Exposed Persons (PEPs) and customers who are close relatives of PEPs and accounts of which PEP is the ultimate beneficial owner
10. Accounts of cash intensive business such as accounts of bullion dealers (including sub-dealers) and jewellers.
11. Customers with dubious reputation as per publicly available information
12. Corporate entities availing secured loans for retail lending or any other activity having no corporate governance and no sound business practices, no proper transaction through banking channels, no robust Board and reputed shareholders and Loss making track record for a period of at least 2 years may also be categorized as high risk.

As part of the AML-KYC policy Re-KYC is to be done for the high-risk customers once in 2 years, for medium risk customers once in 8 years and for low-risk customers once in 10 years.

FIXED DEPOSIT HOLDERS RISK CATEGORISATION

Criteria	Low	Medium	High
Income Slab for Individuals	0 lakh to 10 lakhs	> 10 lakhs to 50 lakhs	> 50 lakhs
Income Slab for Non-Individuals	0 to 5 Cr	> 5 Cr to 50 Cr	> 50 Cr
Customer Profile		Non-resident customers,	Trusts, charities, NGOs, and organizations receiving donations, , Politically exposed persons (PEPs) of foreign origin;
Nature of Business / Profession			Tobacco Merchant, Gems jewelry merchants, Dimond merchants

Annexure II

Officially Valid Documents

As per Para 3 (a) (xiv) of the RBI KYC Master Direction, the 'Officially Valid Document (OVD)' means:

a) the passport;
b) the driving license;
c) the Voter's Identity Card issued by the Election Commission of India;
d) Proof of possession of Aadhaar number
e) job card issued by NREGA duly signed by an officer of the State Government; and
f) letter issued by the National Population Register containing details of name and address.

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.

Provided that 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.

Further Provided that in case the OVD furnished by the customer does not contain 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;

(v) documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India;

(vi) In case, Customer has authenticated the Aadhar through Bio-matric or OTP , a Self declaration can be treated as Current Address Proof.

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

Provided that,

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 licence 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.

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.

Annexure - III

Digital KYC Process

A. 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 MCSL.

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

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

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

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

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

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

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

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

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

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

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

L. The authorized officer of the Company shall check and verify that:-

   (i) information available in the picture of document is matching with the information entered by authorized officer in CAF.

   (ii) live photograph of the customer matches with the photo available in the document.; and

   (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company 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.

Annexure - IV

Customer Identification Requirements - Indicative Guidelines

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

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

Client accounts opened by professional intermediaries

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank shall still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they shall satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It

shall be understood that the ultimate responsibility for knowing the customer lies with the bank.

Accounts of Politically Exposed Persons (PEPs)

MCSL shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

a. The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
b. Reasonable measures are taken by the Company for establishing the source of funds / wealth;
c. the approval to open an account for a PEP shall be obtained from the senior management;
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;

These instructions shall also be applicable to family members or close associates of PEPs.

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face- to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

Annexure - V

Re KYC norms

a) Individuals:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the MCSL, customer's mobile number registered with the MCSL, ATMs, digital channels (such as online banking / internet banking, mobile application of MCSL), 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 MCSL, customer's mobile number registered with the MCSL, ATMs, digital channels (such as online banking / internet banking, mobile application of MCSL), 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, MCSL , at its option, may obtain a copy of OVD or deemed OVD, as defined in Section 3(a)(xiv), or the equivalent e-documents thereof, as defined in Section 3(a)(x), for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the REs in their internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.

iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the MCSL. Wherever required, MCSL may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.

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

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

b) Customers other than individuals:

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

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

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

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

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

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

iv. In order to ensure customer convenience, MCSL may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of MCSL or any committee of the Board to which power has been delegated.

v. MCSL shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the MCSL such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the MCSL where account is maintained, a more frequent periodicity of KYC

updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of MCSL or any committee of the Board to which power has been delegated.

Annexure - VI

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

Transactions that do not make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnishes a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

Accounts with large volume of credits whereas the nature of business does not justify such credits.

Attempts to avoid Reporting/Record-keeping Requirements

a. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
b. Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.
c. An account where there are several cash transactions below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

a. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
b. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
c. A customer who has no record of past or present employment but makes frequent large transactions.

Certain NBFC Employees arousing Suspicion

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.
(ii) Negligence of employees/willful blindness is reported repeatedly.