KNOW YOUR CUSTOMER (KYC)

AND

ANTI-MONEY LAUNDERING

(AML) POLICY

OF

MASSFIN LENDING SERVICES PRIVATE LIMITED

(MASSFIN)

TABLE OF CONTENTS

Glossary

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PMLA	Prevention of Money Laundering Act
PEP	Politically Exposed Person
KYC	Know Your Customer
AML	Anti-Money Laundering
MASSFIN	**MASSFIN LENDING SERVICES PRIVATE LIMITED**
NBFC	Non-Banking Financial Companies
CTR	Cash Transaction Report
STR	Suspicious Transaction Report
FIU – IND	Financial Intelligence Unit – India
CIBIL	Credit Information Bureau (India) Limited
UIDAI	Unique Identification Authority of India
OVD	Officially Valid Document
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest
CDD	Customer Due Diligence
NRI	Non Resident Indian
PIO	Person of Indian Origin
V-CIP	Video based Customer Identification Process
LE	Legal Entity
UCIC	Unique Customer Identification Code

1. INTRODUCTION

The master direction on Know Your Customer (KYC) issued by the Reserve Bank of India **and** Anti-Money Laundering (AML) standards advised all Non-banking financial companies ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board of the company.

In view of the master direction on Know Your Customer **DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016,** with any amendment/re-enactment thereof issued **by** Reserve Bank of India from time to time and Prevention of Money Laundering Act, 2002 ("**Act**") read with the PreventionofMoney-laundering(MaintenanceofRecords)Rules,2005("**Rules**")withanyfurtheramendments/ re-enactments thereof issued from time to time**,** the Board of Directors of **MASSFIN LENDING SERVICES PRIVATE LIMITED** has adopted a policy on Know Your Customer (KYC) &Anti-Money Laundering (AML) norms.

MASSFIN LENDING SERVICES PRIVATE LIMITED(hereinafter referred to as "**the Company**" or **"MASSFIN")** is a Non-Deposit taking Non-Systematically important Non-Banking Finance Company registered with the Reserve Bank of India ("RBI") to carry out the business of a Non-banking financial company with an objective to provide financial assistance to the individuals, MSMEs, and Corporates.

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

2. Objective

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities.

The guidelines also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business,

reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently.

Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

3. KEY DEFINITIONS

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

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

c) "**Board**" means Board of Directors of the Company.

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

e) "**Certified Copy**" means a comparative copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the company.

f) "**Company**" means **MASSFIN LENDING SERVICES PRIVATE LIMITED.**

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

h) **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner

i) "**Designated Director**" means Managing Director or a whole-time Director, or any director duly authorised by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act and the Rules;

Explanation:

1) 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.
2) "Directors" means individual Directors or Directors on the Board of the Company.

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

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

l) **"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.

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

n) **Non-face-to-face Customers**" mean customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

o) "**Officially Valid Document**" (OVD) means Passport, Driving license, Proof of possession of Aadhaar Number, 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 also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India".

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.

p) "**Person**" includes an individual, a Hindu undivided family, a Company, a firm, an association of persons, a body of individuals, whether incorporated or not, or every artificial juridical person, not falling within any one of the above persons any agency, office or branch owned or controlled by any of the above persons.

q) "**Periodic Updation**" means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the Reserve Bank or act or rules.

r) "**Principal Officer**" means an officer nominated by the Company, responsible for furnishing information as per Rule 8 of the Rules;

s) **Politically Exposed Persons ("PEP")** Politically Exposed Persons are Persons who are or have been entrusted with prominent public functions in India or foreign country, e.g., Heads of States or of Governments, senior politicians (eg. MPs, MLAs, MLC, Municipal Counsellors, Panchayat President, Members), senior government/judicial/military officers, senior executives of state-owned corporations, all political party officials, Political Parties, etc.

t) "**Regulated Entities**" (REs) means: all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks(RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs)/State and Central Cooperative Banks (St CBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks' All India Financial Institutions (AIFIs) All Non-Banking Finance Companies (NBFC)s, Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs). All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator

u) "**Suspicious Transaction**" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith: gives rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Schedule to the Act, regardless of the value involved; or appears to be made in circumstances of unusual or unjustified complexity, or appears to not have an economic rationale or bonafide purpose, or gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transactions 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.

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

i. Opening of an account, or
ii. 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; or
iii. The use of a safety deposit box or any other form of safe deposit; or
iv. Entering into any fiduciary relationship; or
v. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
vi. Establishing or creating a legal person or legal arrangement.

w) "**Video-based Customer Identification Process (V-CIP)**" means a method of customer identification by an official of the company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the applicable Master direction on NBFC or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of

Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. KEY ELEMENTS

The Company has framed its KYC policy incorporating the following four key elements:

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

For the purpose of the KYC policy, a 'Customer' is defined as per Clause 3 i.e., Definitions.

a) Customer Acceptance Policy (CAP)

"MASSFIN" lays down criteria for acceptance of customers. While taking the decision to grant any facilities to the customers as well as during the continuation of any facilities the following norms and procedures will be followed by the company

The Customer Acceptance Policy will ensure that explicit guidelines are in place on the following aspects of customer relationship in the Company:

i. No loan account is opened in anonymous or fictitious/benami name(s); The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.
ii. 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 PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
iii. Parameters of risk perception are 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 categorisation of customers into low, medium, and high risk; customers requiring very high level

of monitoring, e.g. Politically Exposed Persons may, if considered necessary, be categorised even higher;

iv. CDD procedure is applied at the unique customer identification number level. This way, if an existing KYC compliant customer wishes to avail another loan from the Company, there will be no need for a fresh CDD exercise.

v. Customers would be categorised as low, medium and high risk.

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

vii. CDD procedure is applied at the UCIC level. This way, if an existing KYC compliant customer wishes to avail another loan from the Company, there will be no need for a fresh CDD exercise.

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

ix. The Company will not open an account or close an existing account where it is unable to apply appropriate customer due diligence measures i.e. it is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non reliability of the data/information furnished to the Company. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, the decision to close an account will be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

x. CDD Procedure is followed for all the joint account holders, co-applicants and guarantor(s) while opening a joint account.

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

xii. Necessary checks will be performed before opening a new loan account to ensure that the identity of the customer does not match with any person with known

criminal background or with banned entities such as individual terrorists or terrorist organizations, UN Security Council List of Prohibited clients. Further, the Company will ensure that the name of the proposed clients does not appear in the consolidated list of individual and entities circulated by the RBI for such purposes.

xiii. A system is required to be put in place for periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers should be carried out at regular intervals as prescribed by Risk Department of the company.

xiv. Where an equivalent e-document is obtained from the customer, the company will verify the digital signature as per the provisions of the Information Technology Act, 2000.

In compliance of above requirements the employees and staffs of the company make sure that the while complying with the aforementioned requirement does not result in any type of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company and the adherence of customer acceptance policy must not result in denial of the company's services to general public, especially to those, who are financially or socially disadvantaged.

b) Customer Identification Procedures

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Company need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship.

1. The first requirement of customer identification procedures to be satisfied is that a prospective customer is the person who he/she claims to be.
2. The second requirement of customer identification procedures is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions.
3. Identity shall be verified for:-

i. The named account holder;
ii. Beneficial owners;
iii. Signatories to an account; and
iv. Intermediate parties.

Copies of the documents produced as Proof of Identity and Address shall be obtained and retained with the Company, wherein a responsible Company Official has to attest such copies certifying that the Originals thereof have been verified.

The periodicity of updating of customer's identification data should be done once in ten years in case of low risk category customers, once in eight years in case of medium risk category customers and once in two years in case of high risk categories.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc).

An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure-A

Also, the information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes.

It will be ensured that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his /her consent and after opening the account.

VIDEO – CUSTOMER IDENTIFICATION PROCEDURE

As per the section 18 of the amended Master Direction on KYC dated 10th May 2021, the company shall undertake V-CIP to carry out the following:

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, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 of the Master Directions on KYC, 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 as per Section 17 of the Master Directions on KYC.

iii. Updation/ Periodic updation of KYC for eligible customers.

Further the Company shall adhere to the minimum standards specified in the Master Directions amendment w.r.t V-CIP infrastructure, procedure, record and data management.

The Company shall take assistance of Banking Correspondents (BCs) in facilitating the V-CIP only at the customer end. However, the company shall maintain the details of the BC assisting the customer, in case the service of BCs are utilized. The ultimate responsibility for customer due diligence will be the Company.

VIDEO – CUSTOMER IDENTIFICATION PROCEDURE

"MASSFIN" may undertake live V-CIP, to be carried out by an official of the **"MASSFIN"**, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the **"MASSFIN"** performing the V-CIP shall record video as well as capture a photograph of the customer present for identification and obtain the identification through Offline Verification of Aadhar.

ii. **"MASSFIN"** shall capture a clear image of the 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.

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

iv. The official of the "**MASSFIN"** shall ensure that the 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.

v. The official of the "**MASSFIN"** 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.

vi. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

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

viii. The audio visual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

ix. **"MASSFIN"** shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

x. **"MASSFIN"** are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the "**MASSFIN".**

xi. **"MASSFIN"** shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

Further, the Company shall adhere to the minimum standards specified in the Master Directions amendment w.r.t V-CIP infrastructure, procedure, record, and data management.

The Company shall take the assistance of Banking Correspondents (BCs) in facilitating the V-CIP only at the customer end. However, the company shall maintain the details of the BC assisting the customer, in case the service of BCs is utilized. The ultimate responsibility for customer due diligence will be the Company.

CUSTOMER DUE DILIGENCE PROCEDURES ("CDD")

The true identity and bonafide of the existing customers and new potential customers opening loan accounts with the Company and obtaining basic background information would be of paramount importance.

Procedure for Obtaining Identification Information

For undertaking CDD, the Company will obtain the information from an **individual,Sole Proprietary Firms, partnership firms, and Legal Entities** 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 related to any legal entity. A detailed procedure to be followed by the Company is attached as **Annexure-B**.

c) Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Since the Company may not have any deposit accounts, this situation will not arise, but the Company shall pay special attention to depleting financial ratios, adequacy of collaterals etc. The Company will put in place a system of half-yearly review of risk categorization of all outstanding accounts and the need for applying enhanced due diligence measures.

The Company must pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Company must also have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity in

order to effectively control and reduce the risk. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should be noted and must be reported.

The Company will ensure that record of transactions in the accounts is preserved and maintained as required under Section 12 of the PML Act, 2002 and Rule 3, 4, and 5 of the PMLA Rules 2005 (Refer Point 8 for maintenance of records and Point 9 for preservation of records under the PML Act) in a separate register at the registered office of the Company in physical or electronic form and make it available to the regulatory and investigating authorities. It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under section 12 of the PML Act, 2002, and Rules 3, 4, and 5 of the PMLA Rules, 2005 is reported to the appropriate law enforcement authority.

d) Risk Management

The Board of Directors of **MASSFIN** has ensured adopt a risk-based approach to ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. The company will adhere to the following for effective implementation of Risk Management.

The Company's internal control and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function will provide an independent evaluation of the Company's policies and procedures, including legal and regulatory requirements.

1. Originals of the KYC documents shall be verified by officials of the Company and copies thereof shall be obtained and retained with the Company. Such copies shall be attested by the Company officials certifying that they have been verified with the originals.

2. KYC documents so obtained shall be properly arranged and filed in order so that they shall be available for verification any time.

3. Company's Internal Auditors/Management shall ensure an independent evaluation of compliance of KYC/AML policy including legal and regulatory requirements. They shall report Lapses observed in this regard as Irregularities in their Audit Reports.

4. Adverse features noted by the Internal Auditors/ Management shall be brought to the attention of the Principal Officer.

5. Summary of serious Irregularities/deviations shall be placed before the Audit Committee of the Board by the Internal Audit Department at quarterly intervals.

6. Review of implementation of KYC/AML guidelines shall also be placed before the Audit Committee of the Board by the Principal Officer at quarterly intervals.

7. The Company shall have an on-going employee training programme so that members of the staff are adequately trained in KYC/AML procedures.

8. The Principal Officer designated by the Company in this regard shall have responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML Policy.

9. Designated Director shall be responsible for the overall compliance with the obligations under the Act and Rules.

RISK PROFILING

1) **"MASSFIN"** to devise a procedure for creating Risk Profiles of their new customers based on risk categorization. The Company shall categorize the customers according to the risk perceived to facilitate undertaking due diligence for the purpose of risk categorization. The customer profile shall contain amongst others information relating to the customer's identity, social/ financial status, nature of the business activity, information about the customer' clients' business and their location, etc.
2) Further, the Company shall seek information from its customers which is relevant for the loan and is in conformity with the guidelines. The customer's profile with the Company shall remain a confidential document and the information shall not be divulged for cross-selling or any other purpose.
3) **MASSFIN** shall categorize the risk profile of individual customers into 2 (two) basic categories in order of the profile. The categories are as below:

Risk Category	Category of Customers
Low Risk Customers	individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as low risk. In such cases, the policy requires only the basic requirements of verifying the identity and location of the customer.
Medium Risk Customers & High-Risk Customers	Customers that are likely to pose a higher than average risk to the Company may be categorised as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. The Company will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

4) The extent of due diligence requirement will vary from case to case as the same will depend upon risk perceived by the Company while granting credit facilities to customers.

5) For the purpose of preparing customer profile only such relevant information from the customers will be sought based on which the Company can easily decide about the risk category in which the customers are to be placed.
6) **"MASSFIN"** has formulated an indicative list of customers and their respective risk categories. The same is attached as **Annexure-C** to this Policy.

PERIODIC UPDATION OF KYC

- As per the requirement of the amended Master Direction on KYC dated 10th May 2021, the Company has adopted a risk-based approach for periodic updation of KYC in the following manner:

S.No.	Basis Risk category	Frequency
1.	High risk customers	Once every two years from the date of opening of the account / last KYC updation
2.	Medium risk customers	Once every eight years from the date of opening of the account / last KYC updation
3.	Low risk customers	Once every ten years from the date of opening of the account / last KYC updation

- The company shall obtain self-declaration from Individual customers and non-Individual customers in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained from customer's registered email id 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.
- The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of Master Direction on KYC, for the purpose of proof of address, declared by the customer at the time of periodic updation.

- In case of change in KYC information of non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

5. DESIGNATED DIRECTOR

MASSFIN shall appoint 'Designated Director' who will be responsible for overall compliance with the obligation imposed under Chapter IV of the PML Act.

6. PRINCIPAL OFFICER

MASSFIN shall appoint 'Principal Officer' who will be responsible for reporting all transactions and sharing of information. He/ She will also be responsible to ensure that proper steps are e taken to fix accountability for serious lapses and intentional contraventions of the KYC guidelines.

Maintenance of records of transactions and reporting.

"MASSFIN" has a system of maintaining a proper record of transactions prescribed under Rule 3 of PMLA rules and transaction, procedure, manner of maintaining transactions, and manner of furnishing prescribed under rule 3, 4, 5, 6, 7 and 8 of PML Rules 2005 mentioned below:

I. All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
II. All series of cash transactions integrally connected to each other which have been valued below rupees ten lakh 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 rupees ten lakh;
III. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
IV. All suspicious 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;
V. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

The records shall be preserved in the following manner:

i) The nature of transactions
ii) The amount of the transaction and the currency in which it was denominated
iii) The date on which the transaction was conducted
iv) The parties to the transaction

The information in respect of the transactions referred to in clauses I, II and III referred above will be submitted to the Director - FIU every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause IV referred above will be furnished promptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.

The information in respect of the transactions referred to in clause V referred above will be furnished promptly by the Director - FIU in writing, or by fax or by electronic mail not later than seven working days on being satisfied that transaction is suspicious.

Strict confidentiality will be maintained by the Company and its employees of the fact of furnishing / reporting details of such suspicious transactions.

As advised by the FIU-IND, New Delhi; the Company will not be required to submit 'NIL' reports in case there are no Cash / Suspicious Transactions, during a particular period.

The required information will be furnished by the Company directly to the FIU-IND, through the designated Principal Officer.

REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA

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

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue

guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Company's Principal Officers, whose all branches are not fully computerised, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

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 misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR 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.

However, robust software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

The Principal Officer can also report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PML rules, 2005 in the prescribed formats at the following address:

Director, FIU-IND,

Financial Intelligence Unit, India,

6th Floor, Hotel Samrat, Chanakyapuri,

New Delhi – 110021

A copy of information furnished shall be retained by the Principal Officer for the purposes of official record.

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.

However, robust software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

7. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

a) The Company 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 will 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, the Company will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

b) The risk assessment exercise by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it will 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 will be available to competent authorities and self-regulating bodies.

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

8. DUE DILIGENCE OF BUSINESS PARTNERS

The following due diligence must also be performed on prospective Business Partners.

A) Verify Identity:

i. Obtain and file legible copies of corporate formation and registration documents or public company prospectuses and government filings.

ii. PAN card of the Directors etc.

iii. Wherever possible (in the case of privately owned entities), arrange for a recommendation from legal counsel to the company.

iv. Wherever possible (in the case of privately owned entities), obtain from appropriate government entity confirmation of due incorporation and existence of the corporation.

V. Wherever possible (in the case of privately owned entities), Verify the identity of All directors, Shareholders, UBO of body corporate through various online sources.

B) Verify Source of Income:

i. Research for the Company details in available news or business databases and obtain all corporate earnings information available.

The Company shall maintain files on each Business Partner with copies of all data obtained and memorialize in writing all the verification efforts. These files may be maintained electronically and should be accessible quickly when needed.

PURPOSEFUL IMPLEMENTATION

The purpose of adopting the above measures and norms while taking decisions on the issue of customer acceptance is twofold. Firstly, the Company should not suffer financially at later stage due to lack of proper due diligence exercise and lack of information which is the exclusive possession of the customers.

a) Secondly, to curb and prevent any such practice by the customers which is aimed to achieve unlawful objectives or any other practice by which the financial institutions can

be used to perpetuate any criminal or unlawful activities. However, at the same time, this policy does not aim or intend to deny the benefit of financial services to those who genuinely need such services / facilities due to real lack of their own sufficient financial resources

9. IDENTIFICATION OF BENEFICIAL OWNERSHIP

The Company will determine the beneficial ownership and controlling interest in case of applicants who are not individuals and the KYC of the beneficial owners will be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice.

Applicable	Guidelines	
Where the client is a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.	a. Ownership of/entitlement to more than 25 % of shares or capital or profits of the company b. Control shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements
Where the client is a partnership firm or a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person	Ownership of/entitlement to more than 15% of the capital or profits of the partnership.
Where no natural person is identified under (i) or (ii) above	The beneficial owner is the relevant natural person who holds the position of senior managing official	

There are certain indicative guidelines issued by RBI from time to time for customer identification requirements for matters such as Trust / Nominee or Fiduciary Accounts, Accounts of companies & firms, Client Accounts opened by professional intermediaries, Accounts of Politically Exposed Persons resident outside India and Accounts of non-face-to-face customers. The Company will adhere to these guidelines to the extent applicable.

10. RECORDS RETENTION

Records pertaining to identification of the customer and their address obtained while opening their loan account and during course of business relationship will be preserved five years from the date of transaction between a client and the reporting entity accordance with the Section 12 of the PLM Act, 2002 and the records mentioned under clause (e) of sub section 1 of PMLA rules 2005 shall retainfor a period of at least five years after the business relationship has ended or the account has been closed, whichever is later.

11. REPORTING TO CENTRAL KYC REGISTRY (CKYCR)

The customer KYC information will be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities (LE)' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

The customer information related to LEs (Legal Entities) will be submitted to CKYCR for accounts of LEs (Legal Entities) opened on or after commencement of NBFI business activities.

Further, during periodic updation, customers' KYC details will be migrated to current Customer Due Diligence (CDD) standards.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and customer will not be required to submit any KYC records unless in the following events:

a) There is a change in information of customer as existing in the records of CKYCR;
b) The current address of customer needs to be verified;
c) It is considered necessary to verify identity or address of customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

KYC Identifier generated by CKYCR will be communicated to the Individual/LE.

12. GENERAL

The Company shall ensure that the provisions of PMLA and the Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

ANNEXURE-A

List of KYC Documents for Different Types of Customers

1. ACCOUNTS OF INDIVIAUAL

A. Permanent Account Number (with photo and signature) or Form 60.

B. One certified copy of an Officially Valid Document (OVD") containing details of the borrower's identity for legal name, and any other names used and address:

- Proof of possession of Aadhaar number in such form as are issued by the Unique Identification Authority of India
- Valid Indian Passport (with photo and signature)
- Valid Voter's ID card issued by the Election Commission of India
- Valid Permanent Driving License (with photo and signature)
- Letter issued by the National Population Register containing details of name and address.

In case of OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVD for limited purpose of proof of address:

- Bank Account Statement
- Letter from any recognised public authority
- Utility Bill not more than two months old (electricity, telephone, post-paid mobile phone, piped gas, water bill) of any service provider
- Property or Municipal tax receipt

A copy of the borrower's marriage certificate issued by the State Government or Gazette notification representing the change in name of the borrower along with a certified copy of the OVD in the existing name of the person shall be obtained for proof of address and identity to establish an account-based relationship or to periodically update records in case the borrower change their names on account of marriage or otherwise.

The following documents may be obtained in addition to OVD subject to the satisfaction of the Company:

1. Property (including land) registration document containing photograph, name, signature and address.
2. Letter from employer (subject to satisfaction of the Company).

Signature Proof:

1. Valid Indian Passport
2. Valid PAN card
3. Valid Permanent Driving license
4. Banker's letter/ verification letter/ ECS verification in original on Bank's letter head bearing the authorising officer's name and signature along with the stamp of the bank. In case the Bank refuses to give the signature verification on the Bank's letter head, then Signature/ ECS verification shall be obtained in the format prescribed for the said purpose.
5. Property registration document containing photograph, name, signature and address

2. Accounts of Proprietary Concerns

1. Permanent Account Number (with photo and signature) or Form 60.

B. One certified copy of an Officially Valid Document (OVD") containing details of the borrower's identity for legal name, and any other names used and address:

- Proof of possession of Aadhaar number in such form as are issued by the Unique Identification Authority of India
- Valid Indian Passport (with photo and signature)
- Valid Voter's ID card issued by the Election Commission of India
- Valid Permanent Driving License (with photo and signature)
- Letter issued by the National Population Register containing details of name and address.

Entity documents:

(i) Proof of the name, address and activity of the entity, like GST certificate or Shop & establishment license or any registration/licensing document issued in the name of the

proprietary concern by the Central Government or State Government Authority/Department.

(ii) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern

3. Accounts of partnership firms

Documents of partner:

(i) Pan card of all the partners.

(i) Address proof as applicable for an individual account.

(ii) The two latest passport size photographs.

Partnership firm Documents:

I. Permanent Account Number of the partnership firm;

II. Proof of the name, address and activity of the entity, like GST certificate or Shop & establishment license or Any registration/licensing document issued in the name of the partnership firm by the Central Government or State Government Authority/Department.

III. Partnership deed

IV. Authority Letter signed by all the partners.

V. The complete Income Tax return of last three years if it is applicable or such lesser period (not just the acknowledgement) in the where the firm's income is reflected duly authenticated/ acknowledged by the Income Tax Authorities.

VI. Utility bills such as electricity, water, and landline telephone bills in the name of the partnership firm.

VII. Any other prescribed equivalent e-documents.

4. Accounts of Companies

I. Basic documents of company i.e. Certificate of incorporation, Memorandum & Articles of Association, Permanent Account Number of the company & Any license or registration certificate by central government state government or any regulatory authority of India.

II. Resolution by the Board of Directors to obtain a loan from **MASSFIN** and authority to any director or employee to act on behalf of the company.

III. One Proof of identity (PAN CARD), Proof of address, and a Colored recent passport size photograph of the authorized person.

IV. List of Directors as on date.

V. List of Shareholders.

VI. Financials statement along with the statutory company's auditor report of the latest preceding completed financial year.

VII. Income tax return of last 3 years or such a lesser period as may be applicable along with the Tax audit report.

VIII. Any other prescribed equivalent e-documents.

ANNEXURE-B

Procedure for Obtaining Identification Information for Undertaking CDD

The Company shall obtain the following information from an individual 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 related to any legal entity:

a) Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. 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 Aadhaar regulations.

b) Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Annexure-B, V-CIP is carried out.

c) If Aadhaar details are used for V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

d) The Company 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.

   ii. Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the

proprietorship firm, as mentioned in Annexure A, apart from undertaking CDD of the proprietor.

iii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication shall be subject to conditions laid down in Master Directions, updated from time to time. i. Updation/Periodic updation of KYC for eligible customers.

iv. Updation/Periodic updation of KYC for eligible customers.

e.) In case the CDD is outsourced, then the records or the information of the customer due diligence carried out by the third party should be obtained within reasonable time from the third party or from the Central KYC Records Registry.

f.) In case the CDD is outsourced, the decision making functions of determining compliance with KYC norms should not be outsourced.

g.) CDD procedure should be applied at the UCIC level and if an existing KYC complaint customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

h.) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have a current address, other current address proof defined under **Annexure-A** shall be obtained from the customer for this purpose.

i.) CDD procedure shall be followed for all joint account holders, while opening a joint account.

j.) The Company can establish relationship with Politically Exposed Persons (PEPs) provided that

a. Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

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

c. the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy; senior level for this purpose shall include HOD & above.

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;

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

ANNEXURE-C

Indicative List for Risk Categorization

High-Risk Customers

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
- Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
- Individuals and entities in watch lists issued by Interpol and other similar international organizations; - Customers with dubious reputation as per public information available or commercially available watch lists; - Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
- Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
- Non-face-to-face customers;
- High net worth individuals;
- Firms with 'sleeping partners';

- Companies having close family shareholding or beneficial ownership;
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff does not constitute physical presence;
- Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the Company;
- Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.;
- Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;
- Gambling/gaming including "Junket Operators" arranging gambling tours;
- Jewellers and Bullion Dealers; - Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);
- Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;
- Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
- Customers that may appear to be Multi-level marketing companies etc;
- Individual, who is a prisoner in jail.

Medium Risk Customers

- Stock brokerage;
- Import/Export;
- Gas Station;
- Car/Boat/Plane Dealership;
- Electronics (wholesale);
- Travel Agency;
- Telemarketers;
- Providers of telecommunications service, internet café, International direct dialling (IDD) call service

Low Risk Customers

All other customers (other than High and Medium Risk category) whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.