KYC and AML Policy -Hari and Company Investments Madras Private Limited

Version	Approval Date	Prepared By	Approved By
Version V1	April 01, 2026	Compliance	Board of Directors

PREAMBLE

The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards, namely **Master Direction - Know Your Customer (KYC) Direction, 2016 ('KYC Directions')** and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the 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 and to prevent itself from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

SCOPE AND APPLICATION OF THE POLICY

1. The scope of this policy is:

   a) To lay down explicit criteria for acceptance of customers.
   b) To establish procedures to identify individuals/non-individuals for opening of account.
   c) To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
   d) To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

2. To fulfil the scope, the following four key elements will be incorporated into our policy:

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

3. Except for Small Accounts as defined in Section 23 of Chapter VI of the KYC Directions, this policy shall also apply to those branches and majority owned subsidiaries of the Company which are located abroad, to the extent they are not contradictory to the local laws in the host country, provided that:

   a) where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the RBI as per the KYC Directions to seek its advise and necessary action for the Company, including application of additional measures to be taken by the Company to manage the ML/TF risks.
   b) in case there is a variance in KYC/AML standards prescribed by the RBI and the host country regulators, branches/ subsidiaries of Company are required to adopt the more stringent regulation of the two.

4. This policy is applicable to all categories of products and services offered by the Company across group level i.e. the Company and its subsidiaries/group entities shall be governed under this Policy, except to the extant where any group entity is subject to KYM-AML provisions of its own. Every Regulated Entity **(RE)** which is part of a group, shall implement programmes/procedures against money laundering and terror financing. The entities in group shall be required to share information

required for the purposes of client due diligence and money laundering and terror finance risk management. However, this shall be carried out with adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

COMPLIANCE WITH THE POLICY

a) The Company shall ensure that compliance with this Policy is being checked in the Internal Audit conducted on the Company.
b) The Company shall ensure that the decision-making functions with respect to KYC-ML matters are not outsourced.
c) All the procedures namely, KYC process, CDD procedure, risk management, customer identification process shall be carried out for all the business verticals across all products without any exception. Any exceptions, if required in any special cases where compliance with the Policy becomes difficult or impossible, shall be approved by the Credit Committee only.

DEFINITIONS – the terms used in this policy shall have the same meaning assigned to them in the KYC Directions and/or the Prevention of Money-Laundering Act, 2002 **(PML Act)** and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 **(PML Rules)**. Few important definitions are provided below:

a) Beneficial Owner (BO) – beneficial owner means:

(i) Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

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.

Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

(ii) 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.

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

(iii) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 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 (i), (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(iv) 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.

b) Certified Copy – Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the PML Act and PML Rules.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, shall be obtained:

(i) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
(ii) branches of overseas banks with whom Indian banks have relationships,
(iii) Notary Public abroad,
(iv) Court Magistrate,
(v) Judge,
(vi) Indian Embassy/Consulate General in the country where the non-resident customer resides.

c) 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 Company as per the provisions contained in the PML Act and PML Rules.

d) Person" has the same meaning assigned in the Act and includes:

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

e) 'Small Account' means a savings account which is opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23 of KYC Directions.

f) Senior Management means and includes the Designated Director and the Principal officer of the Company appointed pursuant to RBI Master Direction.

g) Transaction – means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
(i) opening of an account;
(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;

(iii) the use of a safety deposit box or any other form of safe deposit;
(iv) entering into any fiduciary relationship;
(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.

h) Customer – means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

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

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

j) Non-face-to-face customers – means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company.

k) On-going Due Diligence – means regular monitoring of transactions in accounts to ensure that those are consistent with Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth and other parameters as may be decided by the Credit / Risk committee/function.

l) Periodic Updation – means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI.

m) Policy – means the KYC & AML policy of the Company.

NOTE –

a) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.
b) Wherever the definitions provided under this Policy are contradictory to the provisions of law, the statutory definitions / provisions shall prevail.

CUSTOMER ACCEPTANCE POLICY - guidelines for accepting customers by the Company:

Following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing financial facilities. While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms will be adhered to by the Company:

a) No loan account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account i.e. Benami Account. 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.

b) No Loan account will be opened where HCIMPL is unable to apply appropriate Customer Due Diligence measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer. However, it shall not tip off the customer in any circumstance.

c) The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the concerned officer. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

d) 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 practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by intermediary in a fiduciary capacity.

e) The Company shall not open any account or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:

- The Company is unable to verify the identity of the customer
- The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity
- Information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
- Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.

f) Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

g) The necessary teams shall, at the time of approving a financial transaction/activity, or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the Customer. For co-lending loans, this shall be verified by the NBFC partner at first level. The Company shall however carry out its own checks for KYC verification to the extent possible for independent verification of Customers. The Company shall

also maintain a repository of KYC documents of borrowers under all its products, including the co-lending programme as well. This shall be procured from the third party, if any used, on an immediate basis.

h) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by RBI or other government bodies.

i) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisionps of the Information Technology Act, 2000 (21 of 2000).

j) Wherever required, the Company can obtain / procure additional documents, which may or may not be part of this Policy, but shall ensure to take explicit consent of the Customer for such additional data/information.

k) A Unique Customer Identification Code (UCIC) is allotted while entering into new relationships with customers by the Company. A single customer will not have more than one UCIC.

USAGE OF THIRD PARTY SERVICE PROVIDERS: The Company shall take necessary services of third party service providers in carrying out the KYC process or CDD process, as may be permissible under the KYC Directions.

For the purpose of identifying and verifying the identity of customers 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, the Company may rely on a third party; subject to the fulfilment of conditions as laid down in the KYC Directions.

RISK LEVEL CATEGORIZATION – risk categorization shall take place in line with the guidance provided by the Credit Committee/Board from time to time, which may include the below points provided as guidelines for categorization of customers in different risk categories:

i. The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk. The risk categorization would be a function of the industry the borrower operates in, the geography in which the borrower operates, the shareholding pattern of the entity etc. All Non-Face to Face Customers shall be by default in the High Risk category until their full KYC is carried out either through offline verification or video verification, as per rules prescribed under KYC Directions. Such customers shall be subjected to enhanced monitoring until the identity of the customer is verified through face-to-face mode or V-CIP.

ii. The customer would be classified into risk categories based on the Risk. Further, based on the risk classification a re-KYC needs to be done at a particular frequency. The following guidelines would be suitably modified based on the credit committee approval:

Classification	Guidelines	Frequency **of re-KYC**
High Risk	Any one of the following is met then High Risk ● Document Availability: No PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 and No Aadhar ● AML Checks: AML match ● Type of KYC: Non Face to Face (Digital or CKYC) ● Customers onboarded through E-KYC-Non face to Face will required frequency will be 1 years and limit shall be capped	2 Years
Medium Risk	All of the following to be met then Medium Risk	8 Years

	• Document Availability: Standard KYC (Without Aadhar or PAN or or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962) • AML Checks: non-PEP AML match or no AML Match • Type of KYC: Face to Face	
Low Risk	All of the following to be met then Low risk • Document Availability: PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, Aadhar • AML Checks: No AML match • Type of KYC: Face to Face	10 Years

Note - sub-para (iv) of this section shall also be taken into consideration for determining the risk categorisation of customers.

- *For all the customers where exact AML match for Money laundering cases and Name in the CFT list: should not be onboarded. With review and CC approval such cases can be onboarded on the merits of the case.*

All the customers shall be required to submit Photo or selfie.

iii. The profile of new customers will be prepared on risk categorization basis. Such profile will contain the following information about the new customers:

- Customer's Identity, including identity documents through online or other services offered by issuing authorities
- Social/Legal and financial status of the customer
- Nature of the business activity
- Information about the business of the customer's clients and their locations
- geographical risk covering customers as well as transactions
- type of products/services offered
- delivery channel used for delivery of products/services
- types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions

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

iv. There will be level-wise categorization of customers i.e. Level-I (Low), Level-II (Medium) and Level-III (High). Such levels will be decided based on risk element involved in each case which will be determined by considering the following information submitted by the customer:

- Nature of business of the Customer and of his Clients
- Work place of Customers and of his Clients
- Country of Origin
- Source of funds
- Volume of business six-monthly / annual turn-over
- Social/Legal and financial status
- Quantum and tenure of facility applied for and proposed schedule for repayment of loan
- types of transaction undertaken – cash, cheque/monetary instruments, etc.

v. Customers will be also categorized as high-risk based on the following ML/TF risks:

High Risk Segments/ Sectors

HCIMPL has identified certain segments of clients/ sectors that pose a high risk for ML & TF. These

typically include clients with high physical cash component/ transactions outside of banking channels.

1. Politically Exposed (PEP)
2. Running lottery
3. Gems & Jewellery- this includes companies involved in mining and trading. Would not include entities only involved in shining, polishing, established jewellery stores/ brands and their vendors/ suppliers.
4. Money transfer agencies
5. Forex remittance agencies
6. Crypto currency exchanges/ crypto currency dealers
7. Casino/ gaming

High-Risk Geographic Locations

In addition, Companies that have business locations centered in certain countries have an inherent risk of money laundering and terrorist financing.

Countries that have weak AML frameworks or are susceptible to corruption are more likely to have organizations that conduct illegal activities using their financial systems.

The Financial Action Task Force (FATF) has identified such locations in their website at: "Black and grey" lists and has to be referred to during categorization.

High Risk Products

Given that Hari and Company Investments Madras Private Limited line of business will involve 100% of transactions through formal banking channels; we have not identified any specific products/ services as high risk. If at a later date, there are new products/ services envisaged that involve high usage of physical cash transactions, the same will need to be reviewed and appropriate ML/ TF safeguards will need to be built in.

Identification

Any customer/ potential customer who:

- is from the sectors/ segments/ geographies listed above
- identified from Hygiene or Crime Check or identified from Due Diligence

should be marked as “High Risk ML/ TF”.

Process & Controls

For all such clients, the Credit/ Risk Analysts need to mark client as High Risk from ML/ TF perspective and seek CC approval for onboarding the name with justification/ mitigants/ safeguards. Example: safeguards could include understanding materiality of that business segment as compared to overall size of business, crime check on promoters/ business, market reference check, understanding transaction flow for the client and nature of business, exclusion of funding for certain business segments of the clients, bank statement & GST analysis.

For every annual renewal of such clients, the assessment and safeguards on ML/ TF needs to be refreshed.

vi. Information to be collected from the customers will vary according to categorization of customer from the point of view of risk perceived. However, while preparing customer profile the Company shall seek only such information from the customer which is relevant to the risk category and is not intrusive to the customer. Any other information not specified in the application form, should be sought from the customer separately with his/her explicit consent and after opening the

account.

vii. For risk categorization, individual (other than High Net Worth) and entities whose sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorized as low risk or Level-I category. Normally Level-I customers would be

- Well governed corporates
- Salaried employees having definite and well-defined salary structure,
- Employees of Government Departments or Government owned companies, not considered as PEP
- Statutory bodies,
- Self-employed individuals, however with regular income and good credit behaviour

viii. Cases where the Company is likely to incur higher than average risk will be categorized as medium or high-risk customers and will be placed in medium or high risk category i.e. Level-II or Level-III category. While placing the customers in the above categories, the Company will give due consideration to the following aspects:

- Customer's background,
- Country of his origin,
- Nature and location of his business activities,
- Sources of funds and profile of customer's clients etc.

In such cases, the Company will apply higher due diligence measures keeping in view the risk level.

ix. Special care and diligence will be taken and exercised in respect of those customers who happen to be high profile and/or Politically Exposed Persons ("PEP") within or outside country. Such persons will include:

- Foreign Delegates or those working in Foreign High commissions or Embassies,
- Senior Politicians,
- Senior Judicial Officers,
- Senior Military Officers,
- Senior Executives of State Owned Corporations
- Important political party officials (as explained in Master Direction - Know Your Customer (KYC) Direction, 2016) and
- Family members or close associates of PEPs as mentioned above.

About the accounts of PEPs, in the event of opening of an account for a PEP or in the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, the Company shall obtain Credit Committee's (comprising of the Managing Director, Chief Risk Officer, Chief Credit Officer, Chief Finance Officer) approval in such cases to continue the business relationship with such person, and undertake enhanced monitoring.

x. 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.

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. Ordinarily, the customer profile maintained by the Company will be kept confidential except for cases where the customer himself allows and/or gives consent for the use of the information given in customer profile / application form for offering other products / services of other companies / entities belonging to the Company's group or any other legal entity with whom the Company is having any business tie-ups. However, while taking any such permission or consent of the customer for using his above referred information provided to the Company, it will be ensured that such permission / consent of the customer is unambiguous and explicit.

xi. Cases in which the risk level is higher will require intensive due diligence exercise. Such cases will include those where the sources of funds to be used for business operations or sources to repay the loan to the Company are not clearly disclosed or cannot be ascertained from the financial statements submitted by the customer to the Company. Besides above, some of such customers in whose cases the Company will require higher due diligence measures, especially those for whom the source of funds is not clear, are mentioned below:

- NRI Customers
- Trusts (except trusts appropriately set up under a specific regulation)
- Societies
- Charitable Institutions
- NGOs and other organizations receiving donations from within or outside the country
- Partnership firms with sleeping partners
- Family owned companies
- Persons with dubious or notorious reputation as per the information available from different sources like media, newspapers etc
- Companies having close family shareholding or beneficial ownership
- Politically exposed persons (PEPs) of foreign origin means individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, Senior Politicians, Senior Government, important political officials
- High net worth individuals
- Non-face to face customers

A system of periodic review of risk categorisation of accounts shall be carried out at least once in six months, and the need for applying enhanced due diligence measures shall be further evaluated.

xii. Company shall maintain a record of all anti-money-laundering/terrorism financing-related documents.

DUE DILIGENCE OF BUSINESS PARTNERS – wherever the Company operates through any business partnerships for conducting is business, it shall carry out a due diligence of such Business Partners in the following manner, at time of onboarding and at such periodic interval as may be decided by the Credit Committee, in consultation with such Business Partner.

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 or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 of the Directors etc.
iii. Wherever possible (in the case of privately owned entities), arrange for 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.

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.

In addition to above, adequate due diligence shall be carried for co-lending partners and LSPs as per internally defined mechanism. In cases, where co-lending partners are existing clients of the Company, reliance may be placed on existing procedures and reports. However, the Company shall have a

separate record maintenance for all co-lending partners incorporating background information necessary for conducting due diligence and substantiate the business arrangement.

DUE DILIGENCE ON EMPLOYEES

The Company shall perform the following Due Diligence on Prospective Employees prior to their date of joining

A) Verify Identity:

i. Obtain originals of and file legible copies of identification documents that contain photographs of the individual. Acceptable examples include:

- Passports (obtain all nationalities an individual may have)
- PAN card or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962
- Driver's license
- UID or Physical Aadhaar card/letter or e-Aadhaar letter

B) Verify Domicile of Residence:

i. Example: Obtain copies of utility bill receipts or other form of objective verification of Residence, UID or Physical Aadhaar card/letter or e-Aadhaar letter (if the address provided by the customer is the same on the document submitted for identity proof)

C) Verify the previous year's Employment Record:

i. Obtain and call the previous employer to check the credentials of the prospective employee

ii. Check and verify the address of employee

D) Check References:

i. Obtain 2 or more professional employment references from the prospective employee.

ii. The prospective manager of the employee, or, the Human Resources department, must personally converse with the prospect's references The Company shall maintain files for each employee hired together with copies of all data obtained. These files may be maintained in electronic or physical form and should be accessible quickly when needed.

Further these files will be classified as confidential data and details contained therein shall not be divulged for cross selling or any other purpose.

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.

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.

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

NEED FOR PHOTOGRAPHS

- For all non-individual Customers, photographs of the authorized representatives and directors (excluding independent directors) shall be obtained for all the directors (excluding independent directors) and authorised representatives. These can be part of either customer application form or onboarding journey as part of CDD process.
- In case of change in the authorized signatories, photograph of the new signatory should be obtained duly countersigned by the competent authorities of the concerned institution / organization.
- Where the account is operated by the letters of Authority or Power of Attorney Holder, photograph of the authority holder should be obtained duly attested by the borrower/Customer.

PROOF OF CUSTOMERS' ADDRESS

A detailed list of the features to be verified and documents that may be obtained from the Customers are given in Master Direction - Know Your Customer (KYC) Direction, 2016 of this policy document. A Photostat copy of the proofs should be filed along with the loan application. In case of need, the Company Manager can depute an official to visit the account holder / loan applicant at the given address to satisfy about the genuineness of the address.

CONSULT SANCTIONS LISTS/ FATF STATEMENTS OF KNOWN OR SUSPECTED TERRORISTS AND DEIGNATED LISTS UNDER WEAPONS OF MASS DESTRUCTION (WMD) ACT:

The Company shall ensure that, in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, the Company does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) and whose names appears in the sanctions lists circulated by Reserve Bank of India/. The Company may ensure the aforesaid, verifying the name of person or entity through the website of the concerned entity or through the service provider, who provide the said service of third party verification, in compliance applicable provisions/guideline of Reserve Bank of India/National Housing Bank, the Prevention of Money Laundering Act and rules made thereunder in this regard. Details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list, shall be treated as suspicious and reported to the FIU-IND, apart from advising Ministry of Home Affairs as required under UAPA notification.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services,

business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

The Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list as issued by regulators from time to time.

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

In case of match in the above cases, the Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall also be sent to State Nodal Officer, where the account / transaction is held and to the RBI.

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

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

FREEZING OF LOAN ACCOUNT IN LINE WITH SECTION 51A OF UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967

The procedure laid down by the Government under the UAPA shall be strictly followed and meticulous compliance with the same shall be ensured, as far as applicable.

Specifically, the Company shall ensure compliance with the applicable guidelines requiring it to:

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order, herein after, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the Company shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held by such customer on their books to the Joint. Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone or 011-23092736. The particulars apart from being sent by post, should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.

(iii) The Company shall also send a copy of the communication mentioned in (ii) above to the UAPA Nodal Officer of the State/UT where the loan account is held and the regulators and FIU-IND, as the case maybe.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the Company would prevent designated persons from conducting financial transactions, under intimation to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.

(v) The Company shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted

as per the prescribed format.

(vi) The freeze would apply as appropriate. In case of loan accounts, no further debits shall be permitted. In case of existing deposits, the funds will be frozen.

VIDEO – CUSTOMER IDENTIFICATION PROCEDURE

As per the Clause 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 Clause 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 Clause 17 of the Master Directions on KYC.
iii. Updation/ Periodic updation of KYC for eligible customers.

Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to its exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

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 may rely upon technology provided by any third party but the ultimate responsibility for customer due diligence will be with the Company. The Company shall ensure that the liveliness check while carrying out V-CIP does not result in financial exclusion of person with special needs.

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

PROVISIONS UNDER PMLA

As per the provisions of Rule 9 of the Prevention of Money Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

- At the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship and
- In all other cases, verify identify while carrying out:

  ✓ 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,
  ✓ Any international money transfer operations.

In terms of proviso to rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn.

Abiding by the provisions of Rule 9, the Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The said Rule also require that the Company should exercise ongoing due diligence with respect to the business relationship with every client and closely examine

the transactions to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

Customer identification requirements shall be as per the provisions of the said rule read with KYC Directions.

PERIODIC UPDATION OF KYC

Pursuant to provisions of KYC Directions, 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 in every two years from the date of opening of the account / last KYC updation
2	Medium risk customers	Once in every eight years from the date of opening of the account / last KYC updation
3	Low risk customers	Once in 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 incase of no change in their KYC details. However, incase of change in address of individual customer a self-declaration of such change and proof of new address to be obtained 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 shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in KYC Directions, for the purpose of proof of address, declared by the customer at the time of periodic updation.

Incase 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.

MONITORING OF TRANSACTIONS AND MAINTENANCE OF RECORDS OF TRANSACTIONS

It is equally essential for the Company to have a clear knowledge and understanding about the normal working pattern and activity of the customer so that the Company can identify all such unusual transactions which would fall outside the normal transactions of the customer.

To achieve this purpose, ongoing monitoring is necessary. The extent of such monitoring will depend upon the level of risk involved in a particular account. Any transaction or activity of the customer which gives rise to suspicion will be given special attention. Such monitoring is important to keep a check on any act or omission of the customer which may amount to money laundering or support any act relating to use of finance for criminal activities.

SUSPICIOUS TRANSACTION REPORT (STR)

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted. Throughout this guideline, any mention of a "transaction" includes one that is either completed or attempted.

"Reasonable grounds to suspect" is determined by what is reasonable in the circumstances, including normal business practices and systems within the industry.

There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour.

An illustrative (but not exhaustive) list of suspicious transactions is furnished in "Annexure-1".

Responsibility:

The Compliance Team in co-ordination with the concerned teams should review the STR Reports generated by the AML system and finalize the transactions to be reported as STR. The Compliance Team is responsible for reporting the same to FIU-IND. The AML software has been implemented to monitor suspicious transactions based on criteria defined in the software at a defined frequency. The following activities will be undertaken in the process of reporting suspicious transactions:

- Monitoring of large value and exceptional transactions based on alerts defined
- Liaison with Institutional Business Teams for responses / clarifications on STR alerts
- Escalation of suspicious transactions to respective business heads / product heads
- Filing Cash Transaction Report (CTR) with the FIU by 15th of subsequent month
- Filing Suspicious Transaction Report (STR) with FIU by 15th of subsequent month from date of establishing of suspicious transaction as per the FIU format in both electronic and manual form
- Scrutinizing sample of customer data against UNSCR and other negative lists as issued by Regulatory / Statutory entities from time-to-time and escalating the same to Business Heads.

The Company shall ensure the following:

- carry out an internal Money Laundering and Terrorist Financing risk assessment periodically involving the below mentioned aspects in relation to the onboarded clients
- 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.
- cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time
- be commensurate to the size, geographical presence, complexity of activities/structure, etc. of the clients
- apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.FIU-IND has released a Guidance Note on Transaction Monitoring for NBFCs, which is applicable to the Company as well. Vide the said note, FIU-IND has prescribed certain Red Flag Indicators (RFIs) which are required to be implemented by NBFC for the purpose of generation of alerts to ensure effective transaction monitoring. The Company shall implement these RFIs suitably as may be applicable to its line of business.
- Appropriate thresholds shall be set considering the risk categorization of customers that will ensure intensified monitoring for its customers. While reviewing the alerts, attention shall be paid to the background of the customer, customer's identity, social/financial status, nature of business activity, country of origin, sources of funds, geographical risk, the type of transactions involved, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments,

wire transfers, forex transactions, etc.

CASH TRANSACTION REPORTS (CTR)

All individual cash transactions in an account during a calendar month, where either debits or credit summation, computed separately, exceeding Rupees Ten Lakhs or its equivalent in foreign currency, during the month should be reported to FIU-IND. However, while filing CTR, details of individual cash transactions below Rupees Fifty Thousand may not be indicated.

The Principal Officer should ensure submission of CTR for every month to FIU-IND before 15th of the succeeding month or at such periodicity as may be applicable under the law. CTR should contain only the transactions carried out by the Company on behalf of their clients/customers excluding transactions between the internal accounts of the Company.

COUNTERFEIT CURRENCY REPORT (CCR)

A separate Counterfeit Currency Report should be filed for each incident of detection of Counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident. These transactions should be reported to Director, Financial Intelligence Unit, India by not later than the 15th of the succeeding month from the date of occurrence of such transactions.

All branches of the Company have been provided with machines for detection of fake notes. In the event any fake or counterfeit note is detected by branch staff, despite taking all precautions; then it must be noted in a cash register separately. Reporting of the case with full details like name of customer, amount, denomination, date - must be reported by branch manager to Compliance Department at HO with copy to National Head- Branch Business and Zonal Head.

Compliance to collate all the data and report to NHB / RBI under PMLA, as mentioned above.

MONITORING & REPORTING OF TRANSACTIONS

The Company will keep a continuous vigil, if any of the following acts or events is noticed in relation to the customer's approach or behaviour while dealing with the Company:

1. Reluctance of the customer to provide confirmation regarding his identity

2. Loan money is used for the purpose other than the one mentioned in the sanction letter

form and the real purpose is not disclosd to the Company

3. Customer forecloses the loan prior to the stated maturity

4. Customer suddenly pays a substantial amount towards partial repayment of the loan

5. Customer defaults regularly and then pays substantial cash at periodical intervals i.e. once in six months.

The Company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for a particular category of accounts and pay close attention to the transactions that exceed the prescribed threshold limits. Keeping this in view, the Company shall pay particular attention to the cash transactions which exceed the limits of Rs. 10 lakhs, either per transaction or credit and debit summation in a single month. This would include transaction where the customer by way repayment of loan, whether in part or full, deposit Rs. 10 lakhs and above in cash. Such transactions shall be reported to the Risk Department and the Principal Officer appointed as per this policy. In such cases, the Company shall keep a close and careful watch on the subsequent mode of payments adopted by such customer.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention of the Company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through that account. Company shall ensure that proper record of all transactions and cash transactions (deposits and withdrawals) of Rs.10 lakhs and above in the accounts is preserved and maintained as required under the PMLA.

The Company shall introduce a system of maintaining proper record of the following transactions:

- All cash transactions of the value of more than rupees Ten lakhs to its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below rupees Ten 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 rupees Ten lakhs;
- All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
- All suspicious transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of valuable security or a document has taken place facilitating the transactions;
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

The Company shall ensure that it continues to maintain proper record of all cash transactions (deposits and withdrawals) of Rs. 10 lakhs and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to controlling / head office on a fortnightly basis.

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 Directors, officers and employees of the fact of furnishing / reporting details of such suspicious transactions. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of the KYC Directions of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

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 reporting of the requisite information in respect of cash transactions and suspicious transactions shall be as per the provided formats[1] and shall be in accordance with the reporting guide provided by FIU-IND.

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

[1] https://fiuindia.gov.in/files/downloads/Filing_Information.html#Report_link

High risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such high risk accounts, taking note of the background of the customer, which will include country of origin, source of funds, the type of transactions involved (like accounts having unusual transactions, inconsistent turnover, etc) and other risk factors. Additionally, the Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures basis the revised risk categories.

In addition to the Ordinary Monitoring Standards, any high-risk accounts should also receive the following monitoring:

- Conduct periodic (at least quarterly) reviews of all medium to high-risk accounts
- Create additional reports designed to monitor all transactions in an account to detect patterns of potential illegal activities
- Follow up on any expectations detected from the monitoring reports by contacting the account owner personally to inquire about the unusual activity detected and regularly report status of account inquiries to Compliance Officer.

The Company shall monitor and report such transactions in a manner specified in “Annexure 2”.

RISK MANAGEMENT

I. For effective implementation of KYC policy there will be a proper co-ordination, communication and understanding amongst all the departments of the Company. The Board of Directors shall ensure that an effective KYC program is put in place by establishing proper procedures and ensuring their effective implementation. Heads of all the Departments will ensure that the respective responsibilities in relation to KYC policy are properly understood, given proper attention and appreciated and discharged with utmost care and attention by all the employees of the Company.

II. The Risk department of the Company will carry out quarterly checks to find out as to whether all features of KYC policy are being followed and adhered to by all the Departments concerned. The Risk Department shall sign off on the KYC documents for corporate entities, before every disbursement.

III.'Independent assessment of monitoring procedures

The Company shall also mandatorily include KYC adherence in its internal audit scope every quarter.r. For co-lending partners, the Company shall carry out sample KYC sample audit to assess adherence with the KYC norms.

IV. Company will take steps to ensure that its internal auditors are made well versed with this policy that will carry out regular checks about the compliance of KYC procedures by all the branches of the Company. Any lapse or short coming observed by the internal auditors will be brought to the notice of Department Heads concerned. There will be quarterly assessment to check the compliance level by a committee to be constituted by the Board.

V. Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/ hiring process

shall be put in place.

(b) On-going employee training shall be provided to all the employees to adequately train them in AML / CFT and KYC procedures, related policies, regulations and issues.

VI. The inadequacy or absence of KYC standards can subject the Company to serious risks especially reputational, operational, legal and concentration risks.

a. Reputational risk is defined as the risk of loss of confidence in the integrity of the institution, that adverse publicity regarding the Company's business practices and associations, whether accurate or not causes.

b. Operational risk can be defined as the risk of direct and indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

c. Legal risk is the possibility that law suits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Company.

d. Concentration risk although mostly applicable on the assets side of the balance sheet, may affect the liability as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the liquidity of the Company.

All these risks are interrelated. Any one of them can result in significant financial cost to the Company and diverts considerable management time and energy to resolving problems that arise.

POLICY IMPLEMENTATION GUIDELINES

Customer education

For implementing KYC policy, the Company shall have to seek personal and financial information from the new and intended customers at the time they apply for availing the loan facilities. It is likely that any such information, if asked from the intended customer, may be objected to or questioned by the customers. To meet such situation, it is necessary that the customers are educated and appraised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company. For this purpose, all the staff members with whom the customers will have their first interaction / dealing will be provided special training to answer any query or questions of the customers and satisfy them while seeking certain information in furtherance of KYC Policy. To educate the customers and win their confidence in this regard, Company may arrange printed materials containing all relevant information regarding KYC Policy and anti-money laundering measures. Such printed materials will be circulated amongst the customers and in case of any question from any customer, the Company staff will attend the same promptly and provide and explain reason for seeking any specific information and satisfy the customer in that regard.

Introduction of new technologies

As part of the KYC and AML Policy, special attention should be paid to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favour anonymity and adequate measures, if needed, should be taken to prevent their use in money laundering schemes. The Principal Officer should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

The Company shall ensure:

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

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

Applicability to branches and subsidiaries outside India

The KYC and AML Policy will also apply to the branches and majority owned subsidiaries of the Company located abroad, if any. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought into the notice of RBI.

KYC policy for existing customers

Although this KYC Policy will apply and govern all the new and prospective customers; some of the KYC procedures laid down in this policy particularly which deal with Customer Identification, Monitoring of Transactions and Risk Management can be effectively applied to the existing customers and their loan accounts. While applying such KYC procedures to the existing loan accounts if any unusual pattern is noticed, the same should be brought to the notice of the Department Heads concerned and the Principal Officer appointed by the Company as per RBI directives.

In case any existing customer does not co-operate in providing the information required as per KYC policy or conducts himself in such manner which gives rise to suspicion about his identity or credentials, such matters will be brought to the notice of Principal Officer who in turn will make necessary inquiries and if required shall forward the name of such customers to the authorities concerned for appropriate action. Besides above, in such situation the

Company, for reasons to be recorded, may recall the loan granted to such customers and take recourse to legal remedy against the customers as well as security furnished by such customers.

APPOINTMENT OF DESIGNATED DIRECTOR

A “Designated Director” means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board. (b) The name, designation, contact details and address of the Designated Director shall be communicated to the FIU-IND and RBI. (c) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

APPOINTMENT OF PRINCIPAL OFFICER

To ensure effective implementation of this KYC Policy and a proper co-ordination and communication between the Company and RBI and other enforcement agencies, the Company shall designate a senior official Principal Officer who will operate from the corporate office of the Company. The job of the Principal Officer will be to maintain an effective communication and liaison with RBI and other enforcement agencies which are involved in the fight against money laundering and combating financing of terrorism, and to take appropriate steps in all such matters which are brought to the notice of the Principal Officer by any department of the Company regard to any suspicious acts or omissions or acts of noncompliance on the part of any customers.

The name of the Principal Officer so designated, his designation, contact details and address including changes from time to time, shall be communicated to the Director, FUI-IND and RBI.

Principal Officer shall be located at the Head / Corporate office of the Company. and will be the official responsible for ensuring fraud monitoring and reporting in accordance with Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016 dated September 29, 2016.

MAINTENANCE AND PRESERVATION OF RECORDS

As per the provisions of PMLA, the Company shall maintain records as under:

a) Records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules [referred to in Para 5. Supra] are required to be maintained for a period of ten years from the date of transactions between the Clients and the Company.

b) Records of the identity of all clients of the Company are required to be maintained for a period of ten years from the date of cessation of transactions between the Clients and the Company.

The Company will ensure that the appropriate steps are taken to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copy) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

FRAUD MONITORING AND REPORTING

The Principal Officer is also responsible to continuous monitoring of fraud as per the established monitoring mechanism of the Company and shall ensure submission of all the returns to the Reserve Bank of India and reporting referred to in Master Direction - Monitoring of Frauds in NBFCs (Reserve Bank) Directions, 2016.

REPORTING TO FINANCIAL INTELLIGENCE UNIT - INDIA

The Principal Officer will report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director, FIU-IND,

Financial Intelligence Unit,

India, 6th Floor, Hotel Samrat,

Chanakyapuri,

New Delhi - 110021

Where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of PMLA rules, such officer shall furnish information in respect of such transactions to the Director, FIU-IND, within the prescribed time.

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

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 I

Illustrative list of suspicious activities[2]

Transactions Involving Large Amounts of Cash

i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;

ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

iii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;

iv. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;

v. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;

vi. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;

vii. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;

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

Activities not consistent with the Customer's Business

i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

ii. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.

iii. Unusual applications for DD/TT/PO against cash.

iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.

v. Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid Reporting/Record-keeping Requirements

i. 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.

ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.

[2] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=4246&Mode=0

iii. An account where there are several cash deposits/withdrawals 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

i. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.

ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

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

Customer who provides Insufficient or Suspicious Information

i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

ii. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

iii. A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.

ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.

iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

Certain Bank 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.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans
- Large deposits immediately followed by wire transfers
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts
- Multiple deposits of money orders, Banker's cheques, drafts of third parties
- Transactions inconsistent with the purpose of the account

- Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

- A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
- A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
- A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- A customer experiences increased wire activity when previously there has been no regular wire activity.
- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- A business customer uses or evidences or sudden increase in wired transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
- Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- Periodic wire transfers from a person's account/s to Bank haven countries.
- A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques
- A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when

- The amount is very large (say over Rs.10lakhs)
- The amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any)
- The funds come from a foreign country or
- Such transactions occur repeatedly.

- A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold).

Annexure 2

Process for monitoring and reporting of suspicious transactions

1. Raising suspicion

   When the concerned officer has reason to believe that a transaction is/ may be a suspicious transaction, which may be linked with terrorist activity or money laundering, s/he must flag the issue forthwith to the senior management. The concerned officer may consider the following for the purpose of flagging such issue:

   - Amount involved are related to crimes of money laundering, the financing of terrorism, or the financing of illegal organisations;
   - Amount involved are intended to be used in an activity related to such crimes.

2. Identification and evaluation

   Once the issue is flagged, a formal due diligence is to be conducted to evaluate the suspicion, which shall factor all the attributes and nature of the transaction and in terms of volume, track record, time of transaction, KYC records, behavioural patterns, customer due-diligence information etc.

   Additional details in relation to a client can be obtained to substantiate further information. Once proper documentation is obtained and if the concerned officer is satisfied, the issue shall be closed and recorded.

   Mere presence of an indicator of suspicion does not necessarily always mean that a transaction is suspicious and needs to be reported. When determining whether a transaction is suspicious, consideration to be given to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its due diligence profile. In some cases, patterns of activity or behaviour that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another.

   In case, the concerned officer is not satisfied, it shall be further evaluated, and a formal report shall be submitted to senior management.

3. Reporting of STR

   The senior management may record the reasons therein and evaluate on onward reporting to FIU-IND. Once the senior management is satisfied, that the suspicious transaction is valid and reportable, the same is reported to FIU-IND in accordance with the prescribed formats.

   The fact of furnishing of suspicious transactions shall be strictly kept confidential to ensure that there is no tipping off to the customer at any level.