Know Your Customer (KYC), Anti Money Laundering (AML), Combating Financing of Terrorism (CFT) and Customer Acceptance Policy (CAP)

Equirus Finance Private Limited

Website: www.equirusfinance.com

Approved in the Board Meeting held on: 28th Jan 2026

Document Control

Document review history

Version	Author	Date	Revision
1.0	Manishkumar Jain	23rd Jan 2026	Drafting and approval of policy document

1. SCOPE

1.1 Applicability

The Know Your Customer and Anti-Money Laundering (**the Policy**) applies to **Equirus Finance Private Limited** (hereinafter referred to as '**the Company**' or '**EFPL**').

This Policy requires the Company and each employee to:

- Protect the Company from being used for money laundering or funding terrorist activities;
- Conduct themselves in accordance with the highest ethical standards;
- Comply with the letter and the spirit of applicable Anti-Money Laundering (AML) Laws, and the Company's KYC and AML procedures;
- Be alert to and escalate suspicious activity and not knowingly provide advice or other assistance to individuals who attempt to violate or avoid money-laundering laws, or this Policy; and
- Co-operate with the regulatory authorities and the Financial Intelligence Unit as per the applicable laws.

1.2 Review of Policy

The Policy shall be reviewed atleast annually or as and when required by the applicable rules and regulations.

1.3 Policy Approval

The Policy and any significant changes therein shall be approved by the Board of Directors of the Company.

2. BACKGROUND

Money laundering refers to concealing or disguising the origin and ownership of the proceeds from criminal activity, including drug trafficking, public corruption, terrorism, fraud, human trafficking, and organized crime activities. Terrorist financing is the use of legally or illegally obtained funds to facilitate terrorist activities. Money laundering and terrorist financing may involve a wide variety of financial products, services, and transactions including lending and investment products, and the financing of equipment and other property that could be used to facilitate terrorism and other criminal activity.

Almost any crime with a profit motive can create proceeds that can be laundered. For example, fraud, theft, illegal drug sales, organized crime, bribery, corruption of government officials and human trafficking can create illegal funds that a criminal seeks to convert into legitimate property without raising suspicion. Tax evasion and violations of fiscal laws can also lead to money laundering.

Generally, the money laundering process involves three stages: placement, layering and integration. As illegal funds move from the placement stage through the integration stage, they become increasingly harder to detect and trace back to the illegal source.

- **Placement** is the point where illegal funds first enter the financial system. The deposit of illegal cash into an account or the purchase of money orders, cashier's checks or other financial products is made. Non-bank financial institutions, such as currency exchanges, money remitters, casinos, and check-cashing services can also be used for placement.

- **Layering** After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.

- **Integration** occurs when the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

To address money laundering, the Government of India and other countries around the world have made money laundering a crime and prescribed regulatory requirements for compliance by the banks, financial companies/ institutions and other regulated/ reporting entities to prevent and detect money laundering. In India and in many other countries, it is a crime to engage in a transaction with knowledge that the funds involved in the transactions are from illegal activity. Knowledge includes the concept of 'willful blindness' (failure to make appropriate inquiries when faced with suspicion of wrongdoing) and 'conscious avoidance of knowledge'.

To prevent money-laundering in India and to provide for confiscation of property derived from, or involved in, money-laundering and related matters, the Parliament of India enacted the Prevention of Money Laundering Act, 2002 (**PMLA**), as amended from time to time. Further, necessary Notifications / Rules under the said Act have been published and amended by the Ministry of Finance, the Government of India.

As per the Prevention of Money Laundering Act 2002, the offence of Money Laundering is defined as:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."

The PMLA and rules notified thereunder impose obligation on banking companies, financial institutions (which includes chit fund company, a co-operative bank, a non-banking financial company and a housing finance institution) and intermediaries which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio

manager, investment adviser etc. to verify identity of clients, maintain records and furnish requisite information to Financial Intelligence Unit- India (FIU-IND). The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

In line with the RBI Master Direction - Know Your Customer Directions DBR.AML.BC.No.81/14.01.001/ 2015-16 dated February 25, 2016 and as amended from time to time, the policy have been reviewed.

The KYC and AML Policy has been prepared considering the following 5 key elements:

a) To lay down the criteria for Customer Acceptance (CAP);
b) Risk Management;
c) To lay down criteria for Customer Identification Procedures (CIP);
d) To establish procedures for monitoring of transactions as may be applicable;
e) To develop measures for educating employees and customers in regard with KYC.

3. DEFINITIONS

For the purpose of KYC Norms, definition of various terms used is as under:

3.1 **Aadhaar Number** – Aadhaar Number means "Aadhaar number", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

3.2 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.

3.3 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.

3.4 **Beneficial Owner (BO)** as per PMLA Rules as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

3.5 **Cash Transaction Report (CTR) -** CTR should include the following:

a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency

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

3.7 **Certified copy of OVD** shall mean comparing the copy of officially valid document produced by the customer with the original and recording the same on the copy by the authorised officer of the regulated entity.
Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

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

3.8 **Counterfeit Currency Transaction-** All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine. These cash transactions should also include transactions where forgery of valuable security or documents has taken place.

3.9 **Customer-** For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.10 **Customer Due Diligence (CDD)-** Client Due Diligence as defined under Rule 9 of the Rules and the amendments thereto'.

3.11 **Designated Director-** Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules and shall include:-

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern

d. the Managing Trustee, if the RE is a trust

e. person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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

3.12 Digital KYC-As defined under Section 3 of PMLA Rules, Digital KYC 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. The Company shall not use the services of Business Correspondent (BC) for this process.

3.13 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 (21 of 2000). [Presently, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.]

3.14 **Equivalent e-document**-As defined u/s Section 3 of PMLA rules, 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. Equivalent e- document has also been permitted for accounts of non-individual customer.

3.15 **E-Sign or electronic signatures** are digital signatures that can be applied to electronic documents as per Section 5 of the Information Technology Act, 2000, which explains the legal recognition of electronic signatures. eSign service is an online electronic signature service that can facilitate an Aadhaar holder to forward the document after digitally signing the same provided the eSign signature framework is operated under the provisions of Second schedule of the Information Technology Act and guidelines issued by the controller.

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

3.17 **KYC Templates** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities, as required by the relevant Rules.

3.18 **Non-face-to-face customers-** Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials.

3.19 **Officially valid document (OVD) -** Any document defined under rule 2(1) (d) of the PMLA Rules and the

amendments thereto as officially valid document for verifying identity and proof of address of customers. As on date, OVD means the passport, the Driving License, , proof of possession of Aadhaar number or Aadhaar Card, the Voter's Identity Card, Aadhaar Card issued by the Election Commission of India, Job Card issued by NREGA duly signed by an officer of the State Government, Letter issued by the National Population Register containing details of name and address
Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique identification Authority of India.

However in cases where the customer has submitted proof of possession of Aadhaar number and offline verification cannot be carried out, the Company shall carry out verification through digital KYC process.

Explanation: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address.

b. Where the OVD or equivalent e-document furnished by the customer does not have updated address, the following documents shall be deemed to be OVD's or equivalent e-document for the limited purpose of proof of address:-

i. utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. Property or Municipal Tax receipt;
iii. Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
v. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.
vi. Any other document allowed under the KYC rules and regulations as allowed by the regulator as on date.

c. the customer shall submit OVD or equivalent e-document with current address within period of three months of submitting the documents specified at 'b' above.

Note: *The above documents (deemed OVD) can only be accepted in cases where the current address of borrower has not been updated in OVD (Document issued by Govt. body). In such scenarios, Customer shall submit updated OVD (Address Proof) with current address within a period of three months of submitting the above documents. Same to be marked as PDD in the system. Branch to ensure OVD (Address proof) issued by Govt body with updated address to be documented with a period of maximum 3 months of loan disbursal.*

d. where the OVD or equivalent e-document presented by a foreign national does not contain the details of address, in such case the documents issued by the government departments of foreign jurisdictions and letter issued by the foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD or equivalent e- document 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.

3.20 **Offline Verification**", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, 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. The Company is authorized to carry out Offline Verification of Aadhaar for identification using XML file or Aadhaar Secure QR Code.

3.21 **On-going Due Diligence-** Regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

3.22 **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, the PMLA and the Rules thereunder.

3.23 **Person**- Person" has the same meaning assigned in the Income Tax Act and includes:

a. an Individual;
b. A Hindu Undivided Family;
c. A Company;
d. A Firm;
e. an association of persons or a body of individuals, whether incorporated or not;
f. every artificial juridical person, not falling within any one of the above persons (a to e); and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

3.24 **Politically Exposed Persons**- Individuals who are or have been entrusted with prominent public functions, e.g., Heads of States/Governments, senior politicians, senior government/ judicial/military officers, senior executives of state-owned corporations, important political party officials etc. Broadly it can be categorized into:

a. Foreign PEPs: Individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials

b. Domestic PEPs: Individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials

c. International organization PEPs: persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions

d. Family members are individuals who are related to a PEP either directly or through marriage or similar forms of partnership.

e. Close associates are individuals who are closely connected to a PEP, either socially or professionally.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, has to inform EFPL within 15 working days and obtain Business Head approval to continue the business relationship.

3.25 **Principal Officer (PO)**- An official designated by the Board of Directors of the Company for overseeing and managing the KYC & AML policies and processes. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

3.26 **'Senior Management'** for the purpose of KYC compliance shall include Designated Director, Chief Risk officer, , Business Head, Operations Head, Compliance Officer & Principal Officer (PO).

3.27 **Suspicious transaction** means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or bona fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

3.28 **Transaction-** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
a) opening of an account;
b) entering into any fiduciary relationship;
c) any payment made or received in whole or in part of any contractual or other legal obligation;
d) establishing or creating a legal person or legal arrangement.

3.29 **"UCIC**" means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

3.30 **Video based Customer Identification Process (V-CIP)**-**
Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP. In case Company is opting to undertake V-CIP, shall adhere to the following minimum standard.

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

4. CUSTOMER ACCEPTANCE POLICY (CAP)

In line with the various guidelines issued by RBI on "Know Your Customer Guidelines & Anti Money Laundering Standards" and provisions of the PMLA, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers.

The features of the CAP are detailed below:

a) The Company shall not open any account(s) in anonymous, fictitious or 'benami' name(s).

b) No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.

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

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation will be specified.

e) 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.

f) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer desires to avail another loan from the Company, there shall be no need for a fresh CDD exercise in case of no change of address. UCIC will help the Company to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Company to have a better approach to risk profiling of customers. Branches are required to strictly avoid creating multiple customer IDs while providing new loan facilities.

g) CDD Procedure will be followed for all the joint account holders, while opening a joint account.

h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

i) The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 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, etc. For this purpose, the Company shall maintain lists of individuals or entities issued by RBI, United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious and reported to FIU-IND as required under UAPA notification dated February 2, 2021. The details of such lists are as under:

(i) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List.

(ii) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.

(iii) Other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

(iv) Any other list circulated by Regulatory bodies (eg. RBI, FIU, MCA, SEBI, IRDA, PFRDA, Stock Exchanges, etc.) in India including enforcement agencies (eg. CBI, ED, SFIO, etc.).

j) Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate due diligence.

The nature and extent of basic due diligence measures to be conducted at the time of establishment of account opening/relationship, would depend upon the risk category of the customers and involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the risks posed by the applicant and the applicant's expected use of the Company's products and services from an AML perspective.

k) The Company may rely on third party verification subject to the conditions prescribed by the RBI, the PMLA and the Rules thereunder in this regard.

l) For non-face-to-face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such customers.

m) Relationship/opening of accounts shall be established and the beneficiary of the relationship/account shall also be identified.

n) The information collected from the customer shall be kept confidential.

o) Appropriate Enhanced Due Diligence (EDD) measures shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs) and their family members/close relatives.

p) In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall be adopted.

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. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision.

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

r) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority

The aspects mentioned in the CAP would be reckoned while evolving the KYC/AML procedures for various customers/products. However, while developing the KYC/CDD procedures, the Company shall ensure that its procedures do not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society.

5. RISK MANAGEMENT

5.1 For Risk Management, the Company will have a risk based approach which includes the following:

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

b) Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

c) The customers will be monitored on regular basis with built in mechanism for tracking irregular behavior for risk management and suitable timely corrective action.

5.2 The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise annually 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 and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company in cognizance of the overall sector-specific vulnerabilities. The outcome of the exercise shall be put up to the Board/Audit Committee of the Board and will be made available to competent authorities and self-regulating bodies.

5.3 High and Medium Risk from AML perspective- A customer that is likely to pose a higher than average risk may be categorized high or medium risk depending on background, nature & location of customer, his/ her profile, scale of customer's volume, his/ her financials and social status etc. Due diligence measures will be applied based on the risk assessment. The Company shall apply enhanced due diligence measures for higher risk customers, especially those for whom the sources of funds are not clear.

a) Indicative list of High Risk Customers

i) Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
ii) 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;
iii) Individuals and entities in watch lists issued by Interpol and other similar international organizations;
iv) Customers with dubious reputation as per public information available or commercially available watch lists;
v) Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
vi) 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.;
vii) Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
viii) Non-face-to-face customers;
ix) High net worth individuals with gross Annual Income > Rs.10 crore and net-worth more than Rs. 100 crores (as per declaration in loan application) and is not a salaried person;
x) Firms with 'sleeping partners';
xi) Companies having close family shareholding or beneficial ownership where Company is in existence for less than 3 years or where there is serious qualification in Audit Report for latest financial year;
xii) Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
xiii) 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;

xiv) Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed;

xv) Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.;

xvi) Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;

xvii) Gambling/gaming including "Junket Operators" arranging gambling tours;

xviii) Jewellers and Bullion Dealers;

xix) 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);

xx) Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;

xxi) Customers engaged in industries that might relate to nuclear proliferation activities or explosives;

xxii) Customers that may appear to be Multi-level marketing companies etc;

xxiii) Companies undertaking Forex Business.

b) Indicative list of Medium Risk Customers

i) Stock brokerage;

ii) Import / Export;

iii) Gas Station;

iv) Car / Boat / Plane Dealership;

v) Electronics (wholesale);

vi) Travel agency;

vii) Telemarketers;

viii) Providers of telecommunications service, internet café, International direct dialing (IDD) call service;

ix) High net worth individuals not meeting criteria mentioned in High risk or Low risk;

x) Companies having close family shareholding or beneficial ownership where Company is in existence for 3 years or more.

5.4 Low Risk from AML perspective-

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 identity and location of the customer are to be met.

Illustrative examples of low risk customers could be:

(i) Salaried applicants whose salary structures are well defined;

(ii) People belonging to government departments,

(iii) People working with govt. owned companies, regulators and statutory bodies etc;

(iv) People belonging to lower economic strata of the society whose accounts show small balances and low turnover;

(v) People working with Public Sector Units;

(vi) People working with reputed Public Limited companies & Multinational Companies;

(vii) High net worth individuals who is a salaried person.

6 CUSTOMER IDENTIFICATION PROCEDURES (CIP)

i) The Company shall undertake identification of customers in the following cases:

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

b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;

c. Selling their own products, selling third party products as agents and any other product,and

d. When the Company has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

ii) The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.

iii) The Company will obtain Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN. The PAN details shall be verified from the database of National Securities Depository Limited, the issuing authority for cases in which identification is carried out through V-CIP.

iv) For the customers that are legal person or entities:

i) the Company will verify the legal status for the legal person/ entity through proper and relevant documents;

ii) the Company will understand the beneficial ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

v) Additional documentation may be obtained from the customers with higher risk perception as may be deemed fit. This shall be done having regard but not limited to location (registered office address, correspondence address and other addresses as may be applicable), nature of business activity, repayment mode & repayment track record.

vi) An indicative list of the nature and type of documents/ information that may be relied upon for customer identification is provided in the 'Annexure A' of this Policy. The documents to be accepted by the Company for customer identification shall be based on the regulatory prescriptions from time to time and shall be finalized after approval from the Compliance Officer, Principal Officer & Head- Risk and Credit.

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

a. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC records registry

b. Adequate steps are taken by the Company to satisfy that copies of identification data and other relevant documentation relating to customer due diligence shall be made available from the third party upon request without delay

c. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;

d. The third party shall not be based in a country/ jurisdiction assessed as high risk;

e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

viii) While undertaking customer identification, the Company will ensure that:

a. Decision-making functions of determining compliance with KYC norms is not be outsourced.

b. The customers shall not be required to furnish an additional OVD or equivalent e-document, if the OVD or the equivalent e-document submitted for KYC contains proof of identity as well as proof of address.

c. The customers will not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence will be made by the Company.

d. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as telephonic conversation, positive address verification, Rent agreement, etc.

e. In case of change in the address mentioned on the 'proof of address', fresh proof of address should be obtained within a period of three months.

7. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

7.1 CDD Procedure in case of Individuals

a) The Company will obtain the following documents from an individual or dealing with the individual who is beneficial owner, authorized signatory or the power of attorney holder while establishing an account based relationship:

i) The Aadhaar number where customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act or certified copy of an OVD containing details of identity and address and one recent photograph

The submission of Aadhaar by an individual as a KYC document in cases other than mentioned above cannot be insisted upon. However the individual if so desires, may provide the same out of his own volition. Customers at their option, shall submit one of the OVD's or the equivalent e-document

ii) one certified copy of an OVD or the equivalent e-document as defined above containing details of identity and address;
iii) one recent photograph;
iv) the permanent account number or form no. 60 as defined in Income Tax Rules, 1962, and
v) such other documents pertaining to the nature of business or financial status specified by the Company.

The Aadhaar number shall be mandatorily be obtained alongwith proof of possession of Aadhaar from individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016.

In case customer desirous of availing benefit or subsidy does not have Aadhaar, then he/she shall submit Aadhaar enrolment id alongwith anyone of the below documents:

- Bank or Post office photo passbook
- Voter id card
- Ration Card
- Kishan Photo Passbook
- Passport
- Driving License
- PAN
- MGNREGS job card
- In case of spouse, her husband's or his wife's as the case may be, Employer Photo id card issued by the Government or any public sector undertaking
- Any other photo id card issued by State Government or Union Territory Administration
    - Certificate of identity with Photograph issued by Gazetted Officer on Official letterhead.
    - Health Card issued by Primary Health Centre or Government Hospital.
- Any other document allowed under the KYC rules and regulations as allowed by the regulator as on date.

The specific consent from the customer is obtained for offline verification of Aadhaar.

If customer submits Aadhaar number, to be ensured that customer to redact or blackout first eight digits Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted delivery of financial and other subsidies benefits and services) Act.
The Aadhaar number is not required to be blackout/redacted in case of the customer availing benefit of subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016.

b) The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer. **Submission of PAN or form 60 in lieu of PAN and officially valid document is mandatory for all customers, to the extent applicable, unless it is specifically exempted under any law/act/regulations/notification/circular etc**.

c) A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.;

d) If a person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative as provided at sub-section 77 of Section 2 of the Companies Act, 2013, read with Rule 4 of Companies (Specification of definitions details) Rules, 2014, with whom the person is staying, as the 'proof of address';

Explanation: A declaration from the relative that the said person is a relative and is staying with him/her shall be obtained. Here relative means relative as per Companies Act, 2013.

e) If a customer categorised as 'low risk' expresses inability to complete the documentation requirements on account of any genuine reason, and where it is essential not to interrupt the normal conduct of business, the Company may, at its discretion, complete the verification of identity of the customer within a period of 6 months from the date of establishment of the relationship.

f) In respect of customers who are categorized as 'low risk' and are not able to produce any of the OVDs mentioned, 'simplified procedure' may be applied,

Explanation: During the periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorized as 'moderate or ''high' risk category, then the Company shall obtain one of the six standard OVDs or the equivalent e-documents listed at para 3.10 above for proof of identity and proof of address immediately.

g) If an existing KYC compliant customer of the Company desires to open another account with it, there shall be no need for a fresh CDD exercise provided there is no change in details last provided under the Company's KYC norms.

7.2 Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

a) There must be a specific consent from the customer for authentication through OTP.

b) The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

c) Accounts opened using OTP based e-KYC shall not be allowed for more than one year within which identification as CDD will be carried out.

d) Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per 7.1 above or as per 7.3 (V-CIP) below is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

e) If the CDD procedure as mentioned above is not completed within a year, in respect of borrowal accounts no further debits shall be allowed.

f) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, REs shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

g) The Company shall strictly monitor procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

7.3 V-CIP

(a) The Company may 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, REs 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.

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

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

If the Company is opting to undertake V-CIP, it shall adhere to the following minimum standards:

(b) V-CIP Infrastructure

(i) Company proposes to implement V-CIP through a Software-as-a-Service (SaaS) model, wherein the V-CIP solution is provided by service providers along with the various API integration used for identity verification and document verification. The V-CIP connection and interaction shall originate from the Company's secured network domain, through authenticated and encrypted access to the SaaS platform. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

(ii) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

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

(iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

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

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

(c) V-CIP Procedure

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

(ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

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

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

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

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

a. OTP based Aadhaar e-KYC authentication
b. Offline Verification of Aadhaar for identification
c. KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker

The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

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

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

(viii) The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.

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

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

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

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

(d) V-CIP Records and Data Management

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

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

7.4 Simplified procedure for opening accounts:

In case a person who desires to open an account is not able to produce documents, as specified in Section 16, the Company shall at their discretion open accounts subject to the following conditions:

a) The Company shall obtain a self-attested photograph from the customer.

b) The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

c) The account shall remain operational initially for a period of twelve months, within which CDD shall be carried out.

d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.

e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

7.5 CDD Measures

The Company shall follow CDD measures for opening of accounts. The different types of customers such as Legal entities, Partnership firm, Trust, Unincorporated association or Body of individuals and any juridical persons not specifically covered in any of the above, such as Government or its Departments, societies, universities and local bodies like village panchayats requires specific CDD measures in line with their businesses. The Company shall obtain documents as CDD measure as per the **Annexure - A** listed below.

For explanation purpose any Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and Term 'body of individuals' includes societies.

7.6 Selling Third party products

The Company, if acting as agents while selling third party products as per regulations in force from time to time, will comply with the following aspects:

a) The identity and address of the customer shall be verified as required under its CIP;
b) Transaction details of sale of third party products and related records shall be maintained.
c) Monitoring of transactions for any suspicious activity will be done.

7.7 Enhanced Due Diligence

a) Accounts of non-face-to-face customers: The Company will include additional procedures i.e., certification of all the documents presented, calling for additional documents and the first payment to be effected through the customer's KYC-complied account with another regulated entity for enhanced due diligence of non-face to face customers.

b) Accounts of Politically Exposed Persons (PEPs): The Company will have the option of establishing a relationship with PEPs, provided that:

i) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

ii) the identity of the person shall have been verified before accepting the PEP as a customer;

iii) the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy;

iv) all such accounts are subjected to enhanced monitoring on an on-going basis;

v) 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;

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

The above will also be applicable to accounts where a PEP is the beneficial owner.

For all the customers for which enhanced due diligence "EDD" is required, the Company will conduct the same in line with EDD policy of the group. Any deviation to group EDD policy will be entertained as an exception and will require approval of Principal Officer. Group Policy is enclosed as Annexure-B.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, has to inform EFPL within 15 working days and obtain Business Head approval to continue the business relationship.

7.8 Identification of Beneficial Owner

This guideline as part of Client Due Diligence Policy, is to obtain sufficient information from the clients in order to identify and verify the identity of persons who beneficially own or control the account. The **beneficial owner(BO)** has been defined as per PMLA Rules as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

Process to identify beneficial ownership:

a) who owns more than 25%/15% of the customer depending upon nature of client as discussed below.
b) who has effective control on the customer
c) the persons on whose behalf transaction is conducted.

Hence a beneficial owner is an individual who satisfies any one step or any combinations of the three steps.

Customer Constitution	**Beneficial owners- Percentage threshold on the controlling ownership interest**
Companies	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 person, has/have a controlling ownership interest or who exercise control through other means. *Explanation- For the purpose of this sub-clause-* *Controlling ownership interest" means ownership of/entitlement to more than 25 er cent of the shares or capital or profits of the company.* *Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.* *Note: Where the customer or the owner of the controlling interest is a company listed n a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.*
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 15 per cent of capital or profits of the partnership.

Un-incorporated association or Body of Individual	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals. *Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.*
Trusts	The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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. *Note: In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.*

8. MONITORING OF TRANSACTIONS/ ON-GOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC procedures. The Company shall on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

The Company shall identify transactions large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

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

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule.

Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

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

8.1 Review of risk categorization

The Company will put in place a system of 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. The Company will carry such review of

risk categorization of customers at a periodicity of not less than once in six months.

8.2 Periodic Updation

The Company will conduct periodic updation of KYC documents at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation subject to the following conditions:

(i) Individual Customers:

a) No change in KYC information: In case there is no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email id registered with the Company, customers registered mobile number, digital channels (such as mobile application, website of the Company) or letter etc.

b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer's email id registered with the Company, customers registered mobile number, digital channels (such as mobile application, website of the Company) or letter etc, and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, the Company, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e- documents as mentioned in Annexure-A below for the purpose of proof of address, declared by the customer at the time of periodic updation.

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

(ii) Customers other than individuals:

a) No change in KYC information: In case of no change in the KYC information of the Legal Entity customer, a self-declaration in this regard shall be obtained from the Legal Entity customer through its email id registered with the Company, customers registered mobile number, digital channels (such as mobile application, website of the Company) or letter from an official authorized by the Legal entity in this regard, board resolution etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with us is accurate and shall update the same, if required, to keep it as up-to-date as possible.

b) Change in KYC information: In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

(iii) Additional measures

In addition to the above, the Company shall ensure the following:

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

b) Customer's PAN details is verified from the database of the issuing authority at the time of periodic updation of KYC.

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

d) The Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

9. REPORTING TO FINANCIAL INTELLIGENCE UNIT- INDIA

9.1 In accordance with the requirements under PMLA, the Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

a) Cash Transaction Report (CTR) - If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

b) Counterfeit Currency Report (CCR)- All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

c) Suspicious Transactions Reporting (STR)- The Company will endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to FIU-IND.

The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

The Government of India, Ministry of Finance, Department of Revenue, Financial Intelligence Unit-India, vide its circular dated 10th February 2016 has issued a guidance notes on effective processes of STRs detection and reporting for NBFC which inter-alia provides indicative alerts for suspicious transactions. Please refer Annexure C for the list of indicative alerts.

9.2 Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports-

The Company will maintain utmost confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the FIU-IND/ higher authorities. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

10. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company will capture the KYC information for sharing with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, under the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company will upload the KYC data pertaining to all types of prescribed accounts with CKYCR, as and when required, in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. If an existing CKYC compliant customer of the Company desires to avail top-up/2nd loan and submits KYC Identifier with the Company with an explicit consent to download records from CKYCR, there shall be no need for a fresh CDD exercise except for scenarios where address of borrower has changed and/ or in case of change in Risk Category in system shall be the same of the borrower.

11. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

If applicable to the Company, it will adhere to the provisions of Income Tax Rules 114F, 114G and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take the following requisite steps for complying with the reporting requirements:

a) Register on the related e-filling portal of Income Tax Department as a Reporting Financial Institution;

b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to;

c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H;

d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.;

e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance;

f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

g) In addition to above, other United Nations Security Council Resolutions (UNSCRs) circulated by the Reserve Bank of India in respect of any other jurisdictions/entities from time to time shall also be taken note of.

12. RESPONSIBILITIES OF THE SENIOR MANAGEMENT

12.1 Designated Director- The Company shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director".

12.2 Principal Officer- An official (having knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business) shall be designated as the Principal Officer of the Company. The Principal Officer will responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

12.3 Key Responsibilities of the senior management

i. Allocation of responsibility for effective implementation of policies and procedures. Submission of quarterly audit notes and compliance to the Audit Committee

ii. To ensure compliance with KYC/Anti money laundering (AML) policies and procedures are covered in the scope of concurrent audit/internal audit system

iii. Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under PMLA.

iv. Proper implementation of the company's KYC & AML policy and procedures.

v. Decision-making functions of determining compliance with KYC norms shall not be outsourced.

Roles and Responsibilities:

Sr No.	Process	Responsibility
1	KYC Documentation at the time of customer meet/ interaction and verification of documents with originals	Business
2	Sanction of customers	Risk and Credit
3	Verification of On-boarding Documents	Operations
4	Disbursement of loans	Operations
5	Periodic risk review and internal audit	Risk & Compliance
6	Periodic updation of KYC	Operations
7	Appointment of Principal Officer(AML) & Reporting	Board & Compliance
8	Monitoring & Reporting Obligations	Business, Risk, Operations & Compliance
9	Information of Suspicious /attempted transactions	All employees
10	No tipping off	All employees
11	AML Training	All employees
	Maintenance of Records	
I	Transaction Details	Business/Operations/ Information Technology
II	Customer data, complaints, account files, business correspondence, account recovery details	Business, Operations, Customer Service Information Technology
12	To adhere to the requirements of Compliance policy	All employees

Note:

The name, designation and address of the Designated Director & Principal Officer, including changes from time to time, shall be communicated to the Director, FIU-IND and also to the other regulator.

Internal Auditor to verify the compliance of KYC/AML policies and procedures and the same compliance of the same will be reported to the Audit Committee.

13. RECORD MANAGEMENT

13.1 **Record-keeping requirements-** The Company shall introduce a system of maintaining proper record of transactions at the registered office of the Company, of transaction (nature & value) in such form required under PMLA as mentioned below:

a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency.

c) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions;

d) all suspicious transactions whether or not made in cash; and

e) records pertaining to identification of the customer and his/her address; and

f) should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

13.2 Records to contain the specified information- The records should contain the following information:

a) the nature of the transactions;

b) the amount of the transaction and the currency in which it was denominated;

c) the date on which the transaction was conducted; and

d) the parties to the transaction.

13.3 Maintenance and Preservation of records

a) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions referred in para 13.2 above;

b) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity;

c) records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card etc.) obtained while opening the account and during the course of business relationship would continue to be preserved for at least 5 years after the business relationship is ended;

d) records may be maintained either in hard or soft format.

14. HIRING OF EMPLOYEES, THEIR TRAINING AND EDUCATION OF CUSTOMERS

14.1 **Hiring of Employees and Employee training**- Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.
On-going employee training program will be put in place so that the members of staff are adequately trained in KYC & AML policy.

14.2 Implementation of KYC Procedures requires the Company to seek information which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. To meet such situation, it is necessary that the customers are educated and apprised 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.

15. Procedure for freezing of funds, financial assets or economic resources or related services

- By virtue of Section 51A of UAPA, the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism.

- Reporting entities shall follow the procedure as laid down in the UAPA order issued by the government dated February 02, 2021 for freezing of accounts of designated individuals/entities in case any customer records are matched with that of designated individuals/ entities. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

- Reporting entities shall comply with the procedure prescribed by respective regulators for unfreezing of accounts of 'designated individuals/entities' in case of individuals/entities inadvertently affected by the freezing mechanism, upon verification that the individual/ entity is not a designated individual/entity.

- Reporting entities shall comply with the procedure prescribed by respective regulator for implementation of requests received for freezing of insurance policies of 'designated individuals/entities' without prior notice to the designated persons involved.

16. Adherence to know your customer guidelines by the persons including brokers/agents etc authorized by the Company's.

a) Persons authorized by the Company for collection and/or selling loan related products, their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to the Company.

b) All information shall be made available to the Reserve Bank of India to verify the Compliance with the KYC guidelines and accept full consequences of any violation by the persons authorized by the Company including brokers/agents etc who are operating on their behalf.

17. Secrecy Obligations and Sharing of Information:

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(b) While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy.

(c) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law;
ii. Where there is a duty to the public to disclose;
iii. the interest of bank requires disclosure; and
iv. Where the disclosure is made with the express or implied consent of the customer.

The Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

Annexure A

Indicative List of Customer Identification Documents

Features	Documents
Accounts of individuals (including Karta of HUF) Proof of Identity/ Address	**Mandatory Document** - PAN or the equivalent e-document thereof/ Form 60 (in case of PAN not available) **And** Copy of any one of the Officially Valid Document or equivalent e- document: • Passport (Not Expired) • Voter's Identity Card issued by Election Commission • Driving License (Not Expired) • Job Card issued by NREGA duly signed by an officer of the State Govt. • Letter issued by the National Population Register containing details of name and address • The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number or Aadhar Card or Proof of Possession of Aadhaar Where the OVD or equivalent e-document furnished by the customer does not have updated address, the following documents shall be deemed to be OVD's or equivalent e-document for the limited purpose of proof of address: – Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); – Property or Municipal Tax receipt; – Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; – Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and Where OVD and deemed OVDs obtained from the customer does not have the current address of the customer, following documents shall be obtained as additional document:

	[Note: These documents cannot be replaced as OVD or deemed OVD and can only be treated as additional document for current address proof] Rent Agreement as per below norms: Rent Agreement not allowed to be taken as Residence Address Proof, if the agreement is <6 months old except under below scenarios with Principal officer/Designated Director approval: If borrower has been staying for more than 6 months: a. Rent agreement mentions stay of 6 months or more even if its recently made & b. Permanent address proof documented & c. Positive Resi FI (Stay confirmed) d. Electricity bill of residence having name of Landlord to be documented. OR e. Rent agreement recently made but we have proof of old expired rent agreements of same address. f. Electricity bill of residence having name of Landlord to be documented. g. Positive FCU with the landlord confirming stay. FCU of rent agreement not required. If borrower has recently shifted to the new place, then : a. Rent agreement & b. Permanent address proof documented & c. Positive Resi FI(Stay confirmed) d. Positive FCU of rent agreement. e. Electricity bill of residence having name of Landlord to be documented.
Accounts of Companies	Certified copy of the following documents shall be obtained • Certificate of incorporation; • Memorandum and Articles of Association; • A resolution from the Board of Directors and power of attorney granted to managers, officers or employees to transact on its behalf; and • An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf. *Note: PAN or form 60 in lieu of PAN and other Officially valid document for proof of identity and address of the persons holding an*

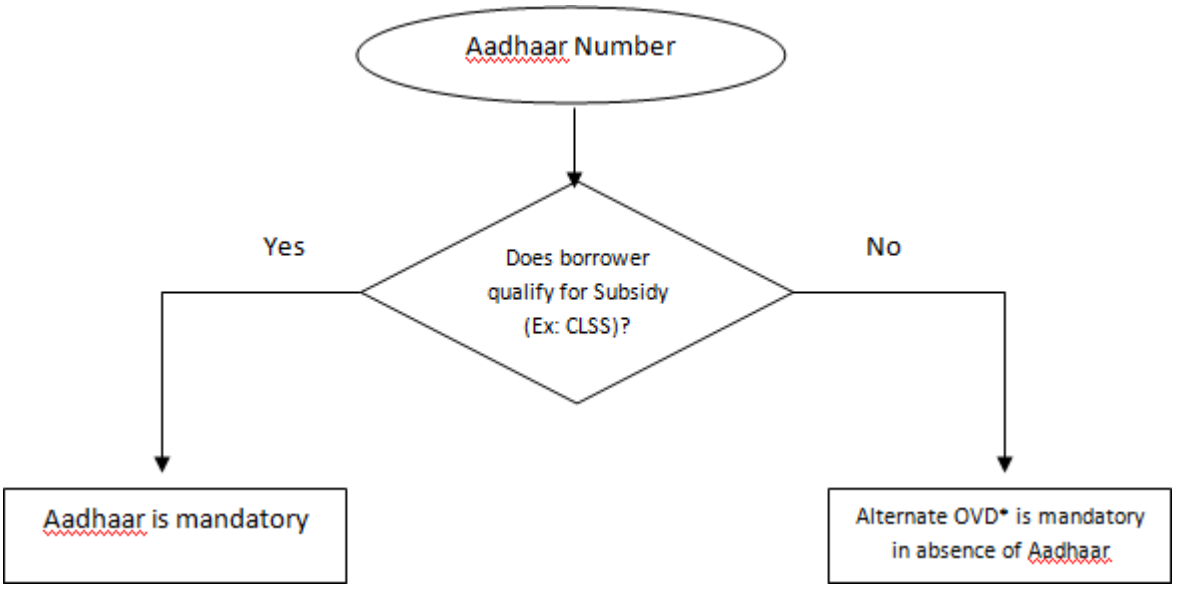
	attorney/authorisation to transact the business on behalf of Company is mandatory. PAN and other Officially valid document for UBO is also required to be obtained.
Accounts of Partnership firms	Certified copy of the following documents shall be obtained • Registration certificate; • Partnership deed; and • An officially valid document in respect of the person holding an attorney to transact on its behalf. *Note: PAN or form 60 in lieu of PAN and other Officially valid document for proof of identity and address of the persons holding an attorney/authorisation to transact the business on behalf of Firm is mandatory.*
Accounts of Trusts and foundations	Certified copy of the following documents shall be obtained • Registration certificate; • Trust deed; and • An officially valid document in respect of the person holding a power of attorney to transact on its behalf. *Note: PAN or form 60 in lieu of PAN and other Officially valid document for proof of identity and address of the persons holding an attorney/authorisation to transact the business on behalf of trust is mandatory.*
Accounts of unincorporated association or a body of individuals	Certified copy of the following documents shall be obtained • Resolution of the managing body of such association or body of individuals; • Power of attorney granted to him to transact on its behalf; • An officially valid document in respect of the person holding an attorney to transact on its behalf; and • Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals. *Note: PAN or form 60 in lieu of PAN and other Officially valid document for proof of identity and address of the persons holding an attorney/authorisation to transact the business on its behalf is mandatory.*
Accounts of Proprietorship Concerns **Proof of the name, address and activity of the concern**	• For opening an account in the name of a sole proprietary firm, a certified copy of an OVD or the equivalent e-document as mentioned above, containing details of identity and address of the individual (proprietor) shall be obtained. PAN or form 60 in lieu of PAN and any other officially valid document of the persons holding an attorney to transact the business on behalf of partnership firm is mandatory.

	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents as a proof of business/ activity in the name of the proprietary concern would suffice: • Registration certificate (in the case of a registered concern) • Certificate/licence issued by the Municipal authorities under Shop & Establishment Act. • Sales and income tax returns • GST Certificate, Certificate/registration document issued by GST/ /Professional Tax authorities • IEC (Import Export Code) issued to proprietary concern by the office of DGFT. • Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities. • Utility bills such as electricity, water and landline telephone bills. *However, in cases where the Company is satisfied that, for any proposal, the proprietary concern is not possible to furnish two such documents, the Company will have the discretion to accept only one of those documents as activity proof. In such cases, the Company, however, will undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the Proprietary concern*.
Accounts of Juridical persons such as Government or its Departments, societies, universities and local bodies like village panchayats	Certified copy of the following documents shall be obtained: Document showing name of the person authorised to act on behalf of the entity; Officially valid documents as mentioned in individual section in Annexure A for proof of identity and address in respect of the person holding an attorney to transact on its behalf; and Such documents as may be required by the RE to establish the legal existence of such an entity/ juridical person. PAN or form 60 in lieu of PAN and other officially valid document of the persons holding an attorney to transact the business on behalf of partnership firm is mandatory.

For Individuals:

1. **PAN Card** is mandatory for every applicant on the loan structure (Income considered and/property owner). Form-60 mandatory for co-applicants whose income is not considered and/ or is not property owner in the absence of PAN.

2. Aadhaar Card:



**OVD is Officially Valid Document. "Officially Valid Document" (OVD) means 'OVD' as defined under the Rule 2(l)(d) of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.*

***Note:** The submission of Aadhaar by an individual as a KYC document in cases other than subsidy cannot be insisted upon. However, the individual, if so desires, may provide the same out of his own wish. Above mentioned documents i.e. PAN & Aadhaar should be documented as a priority and is must in the scenarios as mentioned above. In absence of any of these documents, only if allowed (ex: Aadhaar Card is not mandatory for non-subsidy cases), any alternate document as per OVD list to be taken as ID/ Address proof as applicable.*

Annexure B

Enhanced Due Diligence

The cornerstone of a strong Anti-Money Laundering program is the adoption and implementation of comprehensive customer due diligence policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. As a result, due diligence procedures and processes should be enhanced for such high risk customers. Enhanced Due Diligence (EDD) for High Risk Customers including Politically Exposed Persons (PEPs) is especially critical in understanding their transactions and implementing a monitoring system that reduces the Company's regulatory and reputational risks. High risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship. RBI hasalso continuously emphasised on the need to carry out enhanced due diligence for such high risk customers.

High Risk customer:

A High Risk customer would typically be persons/entities that by nature of their occupation, place of residence or any other characteristic, are more vulnerable to money laundering. Below is the list for classifying a customer as high risk customer

- Non Resident clients
- High Net-worth Individuals (each entity to define threshold for HNI)
- Trusts, Charities, NGOs and organizations receiving donations
- Politically Exposed Persons (PEP) as defined in the AML Policy
- Companies undertaking Forex Business
- Clients in high risk countries where existence / effective money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following - havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
{Note: click the following link for list of high risk countries as published by FATF - *http://www.fatf-gafi.org/countries/#high-risk* }
- Non face to face clients, if any
- Clients with dubious reputation as per public information available etc.

- Apart from above, when establishing business relationship with a customer, the entity should further classify the customer as High Risk/ customer by assessing the following risk categories:

- risk associated with the legal form of the customer (eg. companies having close family shareholding, partnership firm with sleeping partners, etc.);

- risk associated with the economic or personal activity of the customer (eg. person/entity carrying out cash incentive business like restaurant business, dealing in arms, etc.);

- risk associated with the products or services used by the customer (eg. single premium insurance policy where the money is invested in lump sum and surrendered at the earliest opportunity, etc.)

The Company shall exercise independent judgment to ascertain whether any other set of clients shall be classified as High Risk customer or not.

Apart from conducting the basic KYC as per the requirement of the respective business, the entity shall perform EDD for customers who are classified as High Risk Customer.

Enhanced Due Diligence (EDD):

EDD shall comprise the following:

1. **EDD needs to be undertaken at inception of business relationship with a customer.**

- Obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment.

- carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment.

- Laying down reasonable measures to understand whether customer's source of income and net worth is commensurate with the assessed risk of the customer profile. In this regard, any one of the documents as mentioned in **Annexure I** can be obtained. This is an illustrative list and the Credit Team may obtain any additional documents for verifying source of income and net worth in consultation with the Compliance team.

- Basis the above document, Relationship Manager (RM)/Customer facing team to provide report on customer profile. Report to contain customer details like occupation, net worth, income details, beneficial ownership details (in case of non-individual accounts), etc.

Post conducting above due diligence and completion of KYC requirement, approval of senior official shall be taken for on-boarding high risk customer. Operations team in consultation with relationship manager to

provide customer details to the senior official in **Annexure II,** seeking their approval to on-board the customer.

The Company has defined the approval hierarchy for such High Risk customer/.

In the event a customer is identified as a PEP, prior approval of the Principal Officer and Business Head to be taken before onboarding a customer. Post obtaining approval for High Risk customer, customer can be on- boarded, subject to any other business specific requirement.

2. **EDD to be performed during business relationship by taking below steps:**

- More frequent review of the customer's profile/transactions, which shall be more stringent for High risk customer.
- Updation of KYC shall be done at higher frequency for High risk customer accounts as specified by the regulator.

Above EDD process is not intended to be exhaustive, the Company may adopt a more stringent EDD process as per the requirements and regulatory guidelines.

Change in Customer categorisation:

- Where there is change in customer categorisation to high risk basis review of customer's transaction and profile, EDD process as mentioned above shall be carried out.
- Further approval of senior official as per the hierarchy mentioned above shall be taken to continue relationship with such customer.
- In the event, a customer is identified as a PEP, prior approval of the Principal Officer and Business Head to be taken before onboarding a customer.

Annexure I

Illustrative list of Income Proofs

Income proofs for Individuals:

1. Latest copy of Income tax assessment orders/ Income Tax returns slips
2. Form 16 in case of employed individual
3. Latest Salary slip from employer
4. Bank statement showing income credit like salary Income, rent income, etc.
5. Mandi receipt for Agricultural Income
6. CA certificate on client's Income/Net Worth
7. Registered Rent Agreement

Income Proofs for Non-Individuals including HUF:

1. Latest copy of Income tax assessment orders/ Income Tax returns slips
2. Latest copy of Audited Statements
3. Annual Report
4. Chartered Accountant's certificate on client's Income/Net Worth

Annexure II

Basic Client Information	
RM	
RM Code	
RM Entity	
EW Legal Entity	
Customer First Name	
Customer Last Name	
Type of High Risk Customer/ (eg. HNI, NRI, PEP, etc.)	
Why classified as High Risk Customer/ /PEP	
Date of Birth	
Place of Birth	
Address	
National ID/PAN No.	
Other ID	
Passport #	
Action initiated by any enforcement agency	
Are there any sanctions Imposed	
Criminal History if any	
Any adverse news	
Any Additional Information	
Enhance Due Diligence Details	

Customer's Income (as per Income proofs submitted)	
Whether source of income/asset ownership document submitted like ITR, Salary Slip, Form 16, Audited financial statement, etc. (Yes/No)	
Source of Income document submitted by customer independently verifiedYes/No)	
Relationship manager report submitted (Yes/No)	

Basis of recommendation:

Annexure-C

List of RED FLAG INDICATORS (RFI) for STR identification:

Parameter summary

Date wise repayment amount should be filtered based on the 'cash' mode of payment made within a period of 30 days. Different thresholds are specified in the indicative rules against each type of entity i.e. individual, company and other non-individuals and the repayments amount exceeding these thresholds should be considered for alert generation.

Cash entries of repayment exceeding the given threshold in a period of 30 days based on the above mentioned parameters should be reported as STR. The period of 30 days may be within the same month or from 2 consecutive months.

1. **Alert**: Customer whose identity matches with any person whose name figures in the list of banned persons and entities ("Negative lists")

   Parameters for consideration:

   - **Name of Customer:** Name of the applicant, co-applicant, guarantor, security provider and depositor (including joint deposit holder) hereinafter referred to as "Customer" provided in the application (either deposit or Loan), whether individual or entity should be considered before availing any type of services from NBFCs or opening an account with NBFCs.

   - **Negative lists:** Names of the banned/negative entities as mentioned in the UNSCR list published by UN, list published by RBI, Ministry of External Affairs in accordance with Unlawful Activity Prevention Act. 1967 (UAPA) and other lists as mentioned above should be considered for this alert. The updates on these lists are published from time to time and hence the latest lists must be taken into consideration.

   Parameter summary

   Applicants whose names appear in the Negative lists mentioned above should be considered for alert generation.

   As these negative lists are continually updated, it is recommended to conduct the check of existing clients with the additions in the list and matches in the existing Customer database with addition in the negative lists should be considered for generation of alerts and after verification for reporting to FIU.

2. **Alert: Unscheduled High Value repayments in a day:**

Parameters for consideration:

- **Date of Transaction:** Date of transaction is the day on which the payment is recorded. A uniform approach should be observed in arriving at date of repayment in all transaction whether, date of receipt, date of deposit, posting date etc.

- **Type of entity:** The amount threshold prescribed for alert generation in this category differ based on the type of entity and hence entity type should be considered for alert generation when the repayment amount in a day exceeds the threshold for respective entity type.

- **Nature of Payment:** The nature of payment includes all repayments other than the scheduled repayments.

- **Mode of Repayment:** All unscheduled repayments whether cash or non cash repayment should be added to arrive at the total repayment.

Parameter summary

All unscheduled repayments in a day when breaching the prescribed threshold for respective entity type (such as greater than Rs XX* lakh for individuals, greater than Rs. XX* lakh for other entities and greater than Rs. XX* lakh for private and public limited companies) should be considered for alert generation irrespective of mode of payment.

**as decided by the Board of Director depending upon risk profile and other considerations of due diligence / enhanced due diligence as per the extant guidelines in place.*

3. **Alert:** Unscheduled High Value repayments in a calendar month:

Parameters for consideration:

- **Date of repayment and time period:** Date of repayment is the day on which the payment is recorded. A uniform approach should be observed in arriving at date of repayment in all transaction whether, date of receipt, date of deposit, posting date etc.

- **Mode of Repayment:** All unscheduled repayments whether cash or non-cash repayment should be added to arrive at the total repayment.

- **Type of entity:** The amount threshold prescribed for alert generation in this category differ based on the type of entity and hence entity type should be considered for alert generation when the repayment amount in a day exceeds the threshold for respective entity type.

Parameter summary

All unscheduled repayments in a month when breaching the prescribed threshold for respective entity type (such as greater than Rs XX* lakh for individuals, greater than Rs. XX* lakh for other entities and greater than Rs. XX* lakh for private and public limited companies) should be considered for alert generation irrespective of mode of payment.

**as decided by the Board of Director depending upon risk profile and other considerations of due diligence / enhanced due diligence as per the extant guidelines in place.*

4. **Alert:** Splitting of cash transaction just below Rs. 10 lakh by a Customer in a month:

Parameters for consideration:

- **Transaction amount:** Cash transaction amounts which are in the range between Rs. 9,80,000/- and Rs.9,99,999/-.

- **Unique Customer Identification number:** Unique Customer ID which is common across various loans of the same Customer to identify if the repayments across various loan accounts of the Customer.

- **Date of transaction and time period:** Date of transaction is the day on which the payment is recorded. The time period of 30 days should be calculated instead of a calendar month.

- **Mode of Repayment:** Repayments made in only in cash to be considered for this alert type.

Parameter summary

Cash transactions in the range between Rs 9,80,000 and Rs.9,99,999.99 in a single transaction followed by subsequent transaction whether in the same loan or another loan of the same Customer either by cash or non cash should be considered for alert generation as it gives an indication that Customer may have wanted to deposit more than Rs. 10 lakh but possibly to avoid the CTR threshold, the amount was split in one or more transactions within a period of 30 days.

5. **Alert:** Linkage in different loans

Parameters for consideration:

- **Customer Identifier type and reference number:** There are unique identifiers of the Customers such as PAN, Adhar card number, passport number, mobile number, date of birth etc. The value for each of these identifiers should be considered to generate the alert.

- **Customer Name:** Customer opens account with different name but having atleast one common identifiers such as PAN, date of Birth, address etc. should be considered.

Parameter summary:

There are certain identifiers of a Customer which are unique to a Customer such as PAN or date of birth etc. Accordingly any instance where the PAN number of the Customer is same but the name of Customer is different is a case of either a data entry error or misrepresentation. Hence, the instances of same unique identifier being used by two different Customers may be a linkage between the Customers and should be considered for alert generation.

6. **Alert :** High value transactions by High Risk Customers

Parameters for consideration:

- **Transaction amount:** The transaction amount for this alert type is the non-scheduled repayment above Rs.25 lakh whether as part-prepayment, foreclosure or clearance of overdue amount.

- **Risk Grading:** The Risk grade of the Customer to be considered which is as per the KYC Policy of the NBFC based on the regulatory guidelines in accordance with which Customers are classified as High Risk, Medium Risk or Low Risk.

Parameter summary

Single transaction of amount exceeding Rs. 25 lakh by a Customer categorized as a High Risk Customers to be considered for alert generation.

7. **Alert** – information sought by enforcement agencies

i. Occasionally enforcement agencies such as CBI, Police, Enforcement Directorate, Department of Vigilance and Anti-corruption, Income tax or Service Tax Authorities etc. enquire about the statement of account of the Customers.

Normally such alerts should result into STR.

Parameters for consideration

a. Receipt of enquiry notice from any enforcement authority: The notice must be received from any enforcement authority which has statutory powers of enquiry under the applicable laws.

b. Enquiry about a Customer: Such an enquiry must be about a Customer of the Company, seeking information such as statement of account, transaction history, payments made in the account, security created and maturity proceeds etc.

Parameters summary:

Receipt of any notice of enquiry from any enforcement authority, calling for information about any Customer.

NOTE: Where information is sought from the branches a turnaround time needs to be laid down for providing revert to the centralized AML cell. For effective case management all alerts should be closed within defined timelines. All alerts exceeding the timelines should be automatically escalated to the Principal Officer/ his designate.

- **Suspicious & Cash Transaction Reports:** Under the PMLA, STR is required to be submitted not later than seven working days on the Principal Officer being satisfied that the transaction is suspicious.

- **Preservation of records:** All alerts generated and case management for these alerts are required to be preserved for a period as prescribed in the PMLA from the date of transaction or filing of STR whichever is later.

- **Process for filing of STRs through FINnet:** STRs shall be submitted to FIU on the FINnet getway in XML format. The reporting format as well as XML format is available on the FIU website.

- **Periodic audits of the entire monitoring and reporting process:** RBI guidelines mandate audits of the AML process on a periodic basis. It is necessary that the entire process of alert generation, monitoring and reporting of transaction is reviewed independently by internal auditors on a yearly basis (at least) to ensure that the process of monitoring and reporting is effective. Follow up action points arising out of observations relating to transaction reporting under AML needs to be taken as per agreed time frame.