**Aptus Finance India Private Limited**

**Know your Customer (KYC) & Anti Money Laundering (AML) Policy**

## I. Background

In order to safeguard the financial system from being misused as a conduit for Money Laundering and Terrorist Financing, and to preserve its integrity and stability, regulatory frameworks have been continuously strengthened at both international and national levels. Globally, the Financial Action Task Force (FATF), established in 1989, plays a pivotal role in setting standards and promoting the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other related threats. As a member of FATF, India remains committed to adopting and enforcing these international standards to protect the integrity of the global financial system.

At the national level, the legal framework governing Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) is primarily constituted by the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time. These regulations mandate that Regulated Entities (REs) implement robust customer identification procedures at the time of establishing account-based relationships or conducting transactions and undertake ongoing monitoring of such transactions.

In alignment with these requirements, and pursuant to the powers conferred under applicable laws including the Reserve Bank of India Act, 1934, the Payment and Settlement Systems Act, 2007, the Foreign Exchange Management Act, 1999, and relevant provisions of the PML Rules, the Reserve Bank of India (RBI) has issued Know Your Customer (KYC) Directions. These Directions are considered necessary and expedient in the public interest to ensure that financial institutions adopt adequate measures to prevent misuse of the financial system.

Accordingly, this KYC Policy has been formulated to ensure compliance with the applicable regulatory requirements and to establish a robust framework for customer identification, due diligence, and ongoing monitoring, thereby mitigating the risks of Money Laundering and Terrorist Financing.

## II. Objective

The key objectives of the KYC and AML Policy are as under:

(a) To establish a regulatory compliant KYC mechanism to on-board customers;
(b) To ensure compliance throughout the life-cycle of customers as per the laid down norms;
(c) To prevent the Company's business channels/products/services from being used as a channel for Money Laundering ("**ML**")/ Terrorist Financing ("**TF'**);
(d) To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Company;
(e) To ensure compliance with the laws and regulations in force from time to time;
(f) To protect the Company's reputation;

## III. Definitions

1. **"Aadhaar number"** means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act';

2. **"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. **"Beneficial Owner (BO)"** means:
   (a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.
   *Explanation* - For the purpose of this sub-clause:-
      (i) "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
      (ii) "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 agreement.
   (b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership off entitlement to more than 10 per cent of capital or profits of the partnership.
   (c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership off entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

   Explanation- Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
   (d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and other natural person exercising ultimate effective control over trust through a chain of control or ownership.

4. **"Certified Copy"** of Officially Valid Document (OVD) shall mean comparing the copy of the proof of possession of Aadhaar Number where offline verification cannot be carried out or OVD so produced by the customer with the original and recording the same on the copy by the employee of the Company. Such employee will also attest to the duly signed photograph of the customer.

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

6. **"Company"** means Aptus Finance India Private Limited.

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

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

9. **"Customer Identification"** means undertaking the process of CDD.

10. **"Designated Director"** means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money-Laundering Act, 2002 and the Rules there under and shall include the Managing Director or a whole-time Director (as defined under the Companies Act, 2013) duly authorized by the Board.

11. **"Digital KYC"** means that an authorised officer of the Company captures a 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, as per the provisions contained in the Prevention of Money-Laundering Act, 2002.

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

13. **"Equivalent e-document"** means an 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.

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

    Explanation: A customer can obtain his KYC Identifier through the following ways:

    In the process of opening an account, once the customer's KYC Identifier is generated by CKYCR and provided to the Company, the latter shall share the same with the customer concerned. The customer can also access his KYC Identifier on CKYCR Portal (www.ckycindia.in).

15. "**KYC Templates"** means templates prepared to facilitate collating and reporting KYC data to the CKYCR, for individuals and legal entities.

16. "**Non-face-to-face customers"** means customers who open accounts without visiting the branch / offices of the Company or meeting the officials of the Company.

17. **"Officially Valid Document"** (OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, and the letter issued by the National Population Register containing details of name and address. Provided that,
    a) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
    b) Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
        i) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
        ii) property or Municipal tax receipt;
        iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
        iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions, and listed companies and leave and license agreements with such employers allotting official accommodation;

    c) The customer shall submit OVD with a current address within a period of three months of submitting the documents specified at b) above;
    d) Where the OVD presented by a foreign national does not contain the details of address, in such case, the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
    *Explanation:* For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name

18. **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

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

20. **"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 Reserve Bank. The process followed by the Company for periodic updation is explained in this document.

21. **"Person"** has the same meaning as defined in the Act and includes:
    (a) an individual,
    (b) a Hindu undivided family,
    (c) a company.
    (d) a firm,
    (e) an association of persons or a body of individuals, whether incorporated or not,
    (f) every artificial juridical person, not falling within anyone 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).

22. **"Politically Exposed Persons"** (PEPs) are 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.

23. **"Principal Officer"** means an officer nominated by the Company for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law/ regulations, and responsible for communicating and furnishing information to FIU-IND under Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

24. **"Suspicious transaction"** means a "transaction" including an attempted transaction, whether made in cash, which, to a person acting in good faith which:
    (i) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Prevention of Money-Laundering Act, regardless of the value involved; or
    (ii) appears to be made in circumstances of unusual or unjustified complexity; or
    (iii) appears to not have an economic rationale or bonafide purpose; or
    (iv) 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.

25. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
    a) a opening of an account
    b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
    c) the use of a safety deposit box or any other form of safe deposit;
    d) entering into any fiduciary relationship;
    e) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
    f) establishing or creating a legal person or legal arrangement.

26. **"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.

27. **"Video based Customer Identification Process (V-CIP)"** is an alternative method by which an authorised official of the Company conducts customer identification with facial recognition and customer due diligence. This process involves a 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 which the customer furnished, through independent verification and by maintaining an audit trail of the process and the Company shall treat such processes complying with prescribed standards and procedures on par with face-to-face CIP for the purpose of the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025.

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

## IV. Customer Acceptance Policy (CAP)

The Customer Acceptance Policy of the Company, which lays down explicit criteria for acceptance of customers, ensures the following aspects of the customer relationship:

a) The Company shall not open an account in an anonymous or fictitious/ benami name.
b) The Company shall not undertake further transactions like additional disbursements, issuance of cheques/ payment orders, additional Top Up loans etc. (except accepting dues, EMIs and inward funds), with the existing customers/ counter party, if proper KYC documents are not in place.
c) The Company shall not open an account where it is unable to apply appropriate Customer Due Diligence (CDD) either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

d) The Company shall not undertake a transaction or account based relationship without following the CDD procedure. CDD procedure shall also be followed for all the joint account holders while opening a joint account.
e) The Company shall obtain optional/ additional information only with the explicit consent of the customer after undertaking a transaction or establishing an account based relationship.
f) The Company shall obtain the information/documents as specified in this policy under the heading 'customer due diligence procedures for KYC purposes while opening an account and during the periodic updation. However, the documents specified in CDD procedure are in addition to and not in substitution of any other document which the Company may require or is required to obtained under the law for having account based relationship with any legal person or entity including a company, partnership firm, trust, society etc.
g) The Permanent Account Number (PAN), where obtained, shall be verified from the verification facility of issuing authority.
h) A Unique Customer Identification Code (UCIC) shall be allotted while entering into a new relationship with individual customers.
i) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account or desires to avail additional loan facility, there shall be no need for a fresh CDD exercise.
j) The Company shall permit a customer to act on behalf of another person/ entity only in accordance with the law.
k) The Company shall ensure that identity of the customer, directly or indirectly, does not match with any individual terrorist or prohibited/unlawful organisations, whether existing within the country or internationally, or to ensure that the customer or beneficiary is not associated with or affiliated to any illegal or unlawful or terrorist organisation as notified from time to time either by RBI, Government of India, State Government or any other national or international body /organisations. The Company shall maintain a list of individuals or entities issued by RBI, United Nationals Security Council, UAPA or other regulatory & enforcement agencies. Identity of the customer to ensure non-resemblance will be verified from the said list in all the cases before acceptance.

Subject to the above norms and cautions, it will be ensured that the above norms and safeguards do not result in any kind of harassment or inconvenience to bonafide and genuine customers, especially those who are financially or socially disadvantaged, and they should not feel discouraged while dealing with the Company.

In such exceptional circumstances before rejection of service to customers on the issue of his identity, necessary approval from a level senior to the officer normally taking such decision should be obtained.

## V. Customer Identification Procedure (CIP)

Customer Identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data, or information. The Company shall, therefore, obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer /beneficiary of the relationship/account, whether regular or occasional, and the purpose of the intended nature or relationship**.**

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) While entering into the transaction:
   (i) of selling third party products as an agent;
   (ii) of selling the Company's own products and services;
   (iii) for a non-account based customer/ walk-in customer;
   (iv) if the value of a single transaction or series of transactions that appear to be connected is more than rupees fifty thousand.

(d) When it has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-

**Reliance on customer due diligence if done by third party**

The Company for the purpose of verifying the identity of customers, while entering into account based relationship, may rely on customer due diligence done by a third party, subject to the following conditions:

a) Such third party has been duly appointed in writing by the Company for that purpose;
b) 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 the Central KYC Records Registry;
c) Copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available without delay to the Company as and when desired.
d) 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 Prevention of Money-Laundering Act.
e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

## VI. Risk Management

"Risk Management" in the present context refers to money laundering, terrorist funding risk, credit, and financial risks associated with a particular customer from the Company's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by the customer.

For Risk Management, the Company shall have a risk based approach.

a) The Company shall categorize its customers based on the risk perceived by the Company.
b) The Company shall categorize its customers into low, medium, and high-risk category, based on the assessment, profiling, and money laundering risk.
c) The parameters such as customer's identity, social/ financial status, nature of the business activity, and information about the clients' business and their location, etc. shall be considered for risk assessment.
d) The ability to confirm identity documents through online or other services offered by issuing authorities shall also be factored in determining the risk category of the customer.
e) The various other information collected about different categories of customers relating to the perceived risk is non-intrusive and in accordance with this Policy.

The Company will also use FATF Public Statement, the reports and guidance notes issued by Government, RBI, or other authorities on KYC/AML procedures in risk assessment.

The risk categorization has been conducted based on various parameters, including the customer's identity, social and financial status, the nature of their business activities, and information about the client's business and location. Additionally, when assessing the customer's identity, the ability to verify identity documents through online or other services provided by issuing authorities may also be considered.

For a risk based approach, the Company has categorized its customers into three categories as given below.

**I Low Risk**

Individuals and Entities whose identities and sources of wealth can easily be identified and transaction in whose accounts by and large confirm to the known profile come under this category.

i) Salaried employees whose salary structure is well-defined
ii) People belonging to lower economic strata of the society whose accounts show small balances and low turnover
iii) Government Department and Government owned companies, regulators and statutory bodies
iv) Self employed
v) Income Tax assesses

**II Medium Risk**

i) Non-Resident Indians

**III High Risk**

Customers for whom the sources of funds are not clear or are not convincing shall be categorized as High Risk. Higher due diligence shall be applied for this category of customers.

i) Trusts, charities, NGOs and organizations receiving donations
ii) Companies that have close family shareholding or beneficial ownership
iii) Politically exposed persons (PEPs) of Indian/Foreign origin
iv) Non face to face customers
v) Firms with sleeping partners
vi) Those with dubious reputation as per public information available.

The recommendations made by the Financial Action Task Force (FATF) on Anti-money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards shall also be used in risk assessment.

**Money Laundering and Terrorist Financing Risk Assessment by the Company**

The money laundering and terrorist financing risks for the Company are likely to be low due to the following reasons:

a) The Company does not operate in other countries /geographies;
b) The Company does not source/originate loans from other countries/geographies, and its customer base consists of Indian nationals only;
c) The Company extends loans to identified borrowers for which rigorous KYC checks have been put in place;
d) The Company verifies the end use of the loan;
e) The Company does not offer banking, liabilities and insurance products; and
f) The Company offers loans/credit facilities with defined end-use.

The loan disbursements made by the Company is either through electronic bank transfer or through cheques. The Company collects the instalments (EMIs) from customers through NACH/ECS. All pre-closures and part payments made by the customers are accepted only by way of demand drafts/cheques.

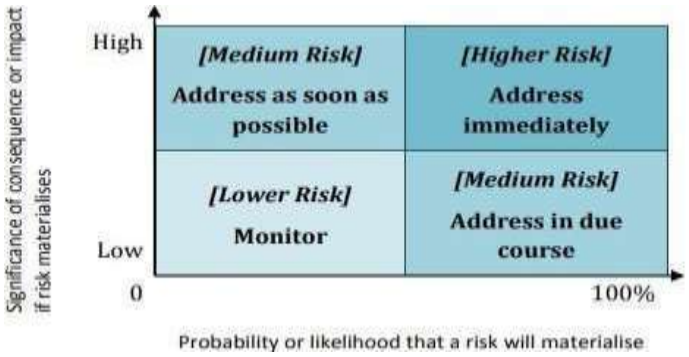
However, the Company will carry out money laundering and terrorist financing exercise periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk to which the Company may be exposed to. Such internal risk assessment shall be commensurate to its size, geographical presence, the complexity of activities/structure, etc.

The exercise undertaken by the Company shall be properly documented, and the assessment process will consider various relevant risk factors and will take cognizance of overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share. Accordingly, it will frame its mitigation plan also. It should involve the relevant functions and have the following stages:

a) **Identification:** Development of a list of potential risk factors drawn from known/suspected threats or vulnerabilities. For this purpose, various important aspects of the KYC Policy (non-compliance of which may pose a threat to Company) will be identified along with the risks which the Company may be exposed to due to the same.

b) **Analysis:** Implementation of key requirements under the KYC Policy should be analyzed. This stage should analyse the likelihood and the impact of each of the identified risks. It will help in assigning priority/ importance to each of the risks.

c) **Evaluation:** It should involve taking the results found during the analysis process to determine priorities for addressing the risks. These priorities should contribute to the development of a strategy for their mitigation. A typical risk evaluation matrix would be as under:




The Company shall conduct the money laundering and terrorist financing risk assessment at least once in a year or at such other intervals as may be decided by the Board.

The outcome of the money laundering and terrorist financing risk assessment will be put up to the Audit Committee.

## VII. Monitoring of Transactions/On-going Due Diligence

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it understands the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. The Company will put in place a process to identify and review complex and unusual transactions/ patterns which have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash or are inconsistent with the normal and expected activity of the customer.

## VIII. Customer Due Diligence (CDD) Procedure

### 1. CDD Procedure in case of individuals

For undertaking CDD in individual cases, the Company shall obtain the following from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

- he/she 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 (18 of 2016); or
- he/she decide to submit their Aadhaar number voluntarily to the Company under the first proviso to sub-section (1) of section 11A of the Prevention of Money Laundering Act; or

(b) the proof of possession of Aadhaar number where the Company can carry out offline verification; or

(c) the proof of possession of Aadhaar number where the Company cannot carry out the offline verification or any OVD or the equivalent e-document thereof containing the details of their identity and address; or

(d) the KYC Identifier with explicit consent to download records from CKYCR;

(a) Permanent Account Number (PAN) OR the equivalent e-document thereof;

(b) Certified copy of one of the OVDs as defined in this policy to be taken for verification of the identity and the address OR the equivalent e-document thereof; and

(c) Other documents including in respect of the nature of the business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company.

**Note:**

(i) If PAN is not available then Form No. 60 as defined in Income-tax Rules, 1962 may be taken;

(ii) Aadhaar Offline Verification: The Company, being a non-bank, may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purposes. However, where its customer submits his Aadhaar number, the Company will ensure such a customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar Act.

If the customer provides an equivalent e-document of any OVD, the Company should verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules made thereunder and take a live photo as specified under Digital KYC Process defined below. The Company may also carry-out KYC verification under Digital KYC Process as defined below.

**2. Digital KYC Process**

In case, Digital KYC Process is adopted by the Company, it will ensure compliance with the following requirements:

(a) It will use an Application to be made available at customer touch points for undertaking KYC of their customers, and the KYC process shall be undertaken only through this authenticated Application of the Company.

(b) The access to such Applications should be controlled by the authorized persons of the Company. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism defined by the Company.

(c) The customer, for the purpose of KYC, shall visit the location of the Authorized Official of the Company ("Authorized Official") vice-versa. The original OVD should be in possession of the customer.

(d) It will be ensured that the live photograph of the customer is taken by the Authorized Official, and the same photograph is embedded in the Customer Application Form (CAF). Further, a water-mark in readable form having CAF number, GPS coordinates, Authorized Official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and timestamp (HH:MM:SS) should be put on the captured live photograph of the customer.

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

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

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

(h) Thereafter, all the entries in the CAF should be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

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

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

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

(l) The Authorized Official should check and verify that: (i) information available in the picture of the document is matching with the information entered by the Authorized Official in CAF. (ii) live photograph of the customer matches with the photo available in the document. and (iii) all of the necessary details in CAF, including mandatory field, are filled in properly.

(m) On Successful verification, the CAF shall be digitally signed by the Authorized Official, who will take a print of CAF, get signatures/thumb-impression of customers at an appropriate place, then scan and upload the same in the system. Original hard copy may be returned to the customer.

**3. Simplified procedure for opening accounts of Individuals**

In case a person who desires to open an account is not able to produce any of the OVDs, the Company may at its discretion open accounts subject to the following conditions:

(a) The Company shall obtain a self-attested photograph from the customer.
(b) The authorized officer of the Company should certify 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 12 months, within which CDD, as prescribed above, should be carried out.
(d) Balances in all their accounts taken together shall not exceed Rs.50,000/- at any point in time.
(e) The total credit in all the accounts taken together shall not exceed Rs.1,00,000/- 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 of Directions (d) and (e) above are breached by him.
(g) When the balance reaches Rs.40,000/- or the total credit in a year reaches Rs.80,000/-, the customer shall be notified 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.

For establishing an account based relationship, the authorized official to ascertain as to whether the customer already has a Customer ID with the Company. In case the customer has an existing Customer ID, the new account shall be opened with the same existing Customer ID.

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

4. **CDD Measures for Sole Proprietary firms**

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

In addition to the above, any two of the following documents or the equivalent e- document thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

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

In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business activity.

Provided, the Company undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

5. **CDD Measures for Legal Entities**

**Partnership Firm:** For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Registration certificate
(b) Partnership deed
(c) Permanent Account Number of the partnership firm
(d) Documents, as specified in paragraph7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

**Company:** For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Certificate of incorporation
(b) Memorandum and Articles of Association
(c) Permanent Account Number of the company
(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
(e) Documents, as specified in paragraph7 above, relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

**Trust:** For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Registration certificate
(b) Trust deed
(c) Permanent Account Number or Form No. 60 of the trust
(d) Documents, as specified in paragraph 7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

**Unincorporated Bodies or associations:** For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Resolution of the managing body of such association or body of individuals;
(b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals;
(c) Power of attorney granted to transact on its behalf;
(d) Documents, as specified in paragraph 7 relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; and
(e) Such additional information as may be required by the Company, to collectively establish the legal existence of such an association or body of individuals.

**Explanation:**

i. Unregistered partnership firms/ trusts shall be included under the term 'Unincorporated associations'.
ii. Term 'body of individuals' includes 'societies'.

**Hindu Undivided Family:** For opening the account of **Hindu Undivided Family,** certified copies of each of the following documents shall be obtained:

(a) Identification information, as mentioned under paragraph 7 in respect of the Karta and Major Coparceners,
(b) Declaration of HUF and its Karta,
(c) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
(d) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

**Juridical Person**: For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Document showing name of the person authorized to act on behalf of the entity;
(b) Documents, as specified in paragraph 7 above, of the person holding an attorney to transact on its behalf; and
(c) Such other documents as may be specified by the Company in writing to establish the legal existence of such an entity/ juridical person.

**Identification of Beneficial Owner**

For opening an account of an entity who is not a natural, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to be undertaken to verify his/ her identity keeping in view the following:

(a) Where the customer or the owner of the controlling interest is a company listed on 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.
(b) In cases of trust/ nominee or fiduciary accounts where 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.

## 6. Periodic Updation

The Company will conduct periodic updation of KYC documents at least once in every 2 years for high risk customers, once in every 8 years for medium risk customers and once in every 10 years for low risk customers in any of the following manner:

i) PAN verification from the verification facility available with the issuing authority. Authentication of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.
ii) In case identification information available with Aadhaar does not contain the current address, an OVD containing the current address may be obtained.

iii) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorised as 'low risk'. In the case of low risk customers, when there is no change in status with respect to their identities and addresses, self-certification to that effect shall be obtained.

iv) In the case of Legal entities, the Company should review the documents sought at the time of opening of the account and obtain fresh certified copies.

v) The Company will not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that the physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/ Consent forwarded by the customer through mail/ post, etc., shall be acceptable.

vi) The Company will provide acknowledgment with the date of having performed KYC updation.

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

**7. Enhanced Due Diligence Process**

(a) **Accounts of non-face-to-face customers:** The Company will ensure the first payment is done through any of the KYC Compliant account through banking channels.

(b) **Accounts of Politically Exposed Persons (PEPs):** If the Company decides to establish a business relationship with PEPs, it will ensure the following:

i) sufficient information including information about the sources of funds of PEPs is gathered;

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 procedures;

iv) all such accounts will be classified as High Risk and will be subjected to required due diligence and monitoring, as applicable;

v) if it gets confirmed to the Company that an existing customer or the beneficial owner of an existing account has subsequently become a PEP, an approval from a senior official of the Company will be obtained to continue the business relationship;

vi) further, such existing accounts that get classified PEPs subsequently will be subjected to enhanced due diligence, as applicable.

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

## 8. Record Management

(a) **Record-keeping requirements:** The Company shall ensure the maintenance of proper record of transactions required under PMLA as mentioned below:

i) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of the transaction;

ii) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of the business relationship, for at least five years after the business relationship is ended;

iii) make available the identification records and transaction data to the competent authorities upon request;

iv) introduce a system of maintaining a proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

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

vi) 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;

vii) 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;

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

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

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

(b) The records should contain the following information:

i) the nature of the transactions;

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

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

iv) the parties to the transaction.

## 9. Reporting requirement to Financial Intelligence Unit-India (FIU-IND)

In accordance with the requirements under the 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. Additionally, the Company will submit 'Statement showing the details of Counterfeit Banknotes detected' to the NHB within 7 days from the last day of the respective quarter. Even in the case of 'Nil' instance also, the statement is to be submitted to the NHB.

(c) Suspicious Transactions Reporting (STR): The Company will monitor 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 the 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.

It has been advised by the FIU-IND, New Delhi, that HFCs need not submit 'NIL' reports in case there are no Cash/Suspicious Transactions, during a particular period.

The Company will maintain confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the FIU-IND/ higher authorities and ensure that there is no tipping off to the customer at any level.

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

## 10. Secrecy Obligations and Sharing of Information

Officials of the of the Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer and requests for data/information from Government and other agencies, the Company shall first satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in mutual dealing except in following circumstances:

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

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

The Company shall not use the information collected from the customer for the purpose of cross selling or for any other purpose without the express permission of the customer.

**11. Sharing KYC Information with Central KYC Records Registry (CKYCR)**

The Company will capture the KYC information/ details as per KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

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

The Company, if applicable, 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 requisite steps for complying with the reporting requirements in this regard.

**13. Compliance with Section 51A of Unlawful Activities (Prevention) Act, 1967**

The Company will ensure compliance with Section 51A of UAPA Act, 1987 by screening the prospective and existing account holders for UN Sanction List or any other list as per UAPA Act, 1987. In the event, any account holder resembles the name of asper the list, it will be reported to FIU-IND and Ministry of Home Affairs. Further, other requirements including the freezing of assets, shall be followed by the Company.

**14. Adherence to the KYC and AML guidelines by the Company's agents**

(a) The Company's agents or persons authorized by it, for its business, will be required to be compliant with the applicable KYC & AML Guidelines.
(b) All requisite information shall be made available to the RBI/ National Housing Bank to verify the compliance with the applicable KYC & AML Guidelines.
(c) The books of accounts of persons authorized by the Company, including agents, etc., so far as they relate to the business of the company, shall be made available for audit and inspection whenever required.

**15. Selling third party products**

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

(a) identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 4 of this Policy.

(b) transaction details of the sale of third party products and related records shall be maintained as prescribed.

(c) Anti-money Laundering (AML) software capable of capturing, generating and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:

(i) debit to customers' account or against cheques; and

(ii) obtaining and verifying the PAN given by the account based as well as walk-in customers.

**16. Quoting of PAN**

Permanent Account Number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

**17. Customer Education**

Seeing of certain KYC information from customers can sometimes lead to queries from the customer as to the motive and purpose of collecting such information. In this regard, the Company will take appropriate steps to educate customers on the objectives of the KYC measures.

**18. Hiring of Employees and Employee Training**

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in the KYC Policy. The focus of the training will be different for frontline staff, compliance staff, and staff dealing with new customers.

**19. Designated Director, Director, Principal Officer and Senior Management, internal audit.**

(a) Designated Director

Mr. P. Balaji, Director of the Company has been nominated by the Board and has been appointed as 'Designated Director' to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. Designated Director, in consultation with the Principal Officer, shall be responsible for setting up the policies for implementation of the KYC program and shall issue subsidiary policies or documents for operationalizing the policy. Designated Director shall allocate responsibilities of officials/departments for ensuring compliance with the KYC Policy.

(b) Principal Officer

Mr. Anto Abinash, Company Secretary & Compliance Officer has been designated as 'Principal Officer'. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The Principal Officer shall assist the Designated Director for setting up various policies for implementation of the KYC Program**.** The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

(c) Senior Management

Senior management for the purpose of KYC compliance shall mean Designated Director, Principal Officer, and head of each department in the Company**.** The Senior Management shall assist the Principal Officer/Designated Director in the effective implementation of the KYC Program and submit compliance status report to them.

(d) Internal Audit

The quarterly audit notes and compliance status shall be submitted to the Audit Committee**.** The audit findings and compliance thereof will be put up before the Audit Committee of the Board till the closure of findings.

**20. Review of Policy**

The policy shall be reviewed annually by the Board of Directors. Any amendment to the policy considered necessary for effective implementation of the KYC Program any time during the year shall be carried out by the Designated Director and shall be placed for ratification at the next meeting of the Board.

**21. Technology**

The Company shall endeavor to use the latest available technology for determining and ensuring compliance with KYC norms.

**22. No outsourcing of decision making function**

The Company shall not outsource decision-making functions of determining compliance with KYC norms.

. **********