KYC AND ANTI MONEY LAUNDERING POLICY

Exclusive Leasing and Finance Private Limited
(Formerly known as Exclusive Leasing and Finance Limited)
CIN: U65921DL1984PTC018746
Regd. Off: 321 & 322, 3rd Floor, Narain Manzil Building, 23,
Barakhamba Road, Connaught Place, New Delhi-110001
Tel: +91 9717623830
Website: www.ezcapital.in

Version	Date of Approval/ Reviewal
V.1	08/04/2022
V.2	10/05/2023
V.3	10/04/2024
V.4	08/04/2025

INDEX

1. INTRODUCTION

Exclusive Leasing and Finance Private Limited (ELFPL) (hereinafter called as 'Regulated Entity/ RE') is focused on meeting the financial needs of the society India who do not have easy access to finance and which has remained largely underserved despite several initiatives.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of Exclusive Leasing and Finance Private Limited (herein after referred to as 'Company') is approved by the Board of Directors. This policy is applicable to all categories of products and services offered by the Company.

The above guidelines shall also apply to the all branches and offices of ELFPL.

2. OBJECTIVE

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all Non-Banking Financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies. In view of the same, ELFPL has adopted the said KYC guidelines with suitable modifications depending on the business activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures be formulated in line with the prescribed RBI guidelines and put in place duly approved by its Board of Directors.

3. REGULATORY FRAMEWORK

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. REs shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s).

The Reserve Bank of India (RBI) vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25 2016 & Master Direction – Reserve Bank of India (Non- Banking Financial Company – Scale Based Regulations) Directions, 2023 dated 10th November, 2023 and subsequent modifications thereof, have prescribed guidelines "Anti Money Laundering" guidelines/ standards.

The Broad objectives are as below:

a) Prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities.

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

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

c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

d) To comply with applicable laws and regulatory guidelines.

e) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

4. DEFINITIONS

A. Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i. "**Aadhaar number**" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. "**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.

iii ."**Authentatio**n", 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

iv. Beneficial Owner (BO)

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

   Explanation- For the purpose of this sub-clause-

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

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

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 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 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.

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 any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. Customer

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

vi. Customer Due Diligence (CDD) - Identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents (OVD)' as a 'proof of identity' and a 'proof of address

vii. Customer identification - means undertaking the process of CDD.

viii. Officially valid document (OVD)

Passport, Driving license, PAN card, Voter ID / Election ID card, Job card issued by NREGA duly signed by an officer of the State Government, and Aadhaar Card / letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Provided that where 'simplified measures' are applied for verifying the identity of the customers the following documents shall be deemed to be OVD:

i. identity card with applicant's photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

ii. Letter issued by a Gazetted officer, with a duly attested photograph of the person.

Provided further that where 'simplified measures' are applied for verifying, for the limited purpose of, proof of address the following additional documents are deemed to be OVDs:

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 Bank account or Post Office savings bank account statement;

iv Pension or family Pension payment orders (PPOs) issued to retired employees by Government Departments or PSUs, if they contain address.

v 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 vi. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.

ix. Person" - means 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)

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

xi. Certified Copy- Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Company as per the provisions contained in the Act. Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 [FEMA 5(R)], alternatively, the original certified copy, certified by any one of the following, may be obtained:

- Authorized 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

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

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

xiv. **Equivalent e-documents-** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 (as amended from time to time, including any statutory modification(s) or re-enactment(s) thereof, for the time being in force).

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

xvi. "**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).

xvii. "**Non-profit organisations" (NPO)** means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xviii. **"Senior Management"** means Chief Executive Officer (CEO), Chief Risk Officer (CRO), Chief Operations Officer and Head of Operations & Credit.

5. KEY ELEMENTS

KYC procedures also enable us to know/understand our customers and their financial dealings better which in turn help them manage their risks prudently. We have framed our KYC policy incorporating the following four key elements:

- Customer Acceptance Policy
- Customer Identification Procedure
- Monitoring of Transaction and
- Risk Management

For the purpose of KYC policy, a "customer" will be defined as:

- Any person or entity connected with 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.

- A person or entity that maintains an account and/or has a business relationship with Company.
- The one on whose behalf the account is maintained (i.e. the beneficial owner).
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law.

6. STRUCTURING OF TRANSACTIONS

The Company shall undertake customer identification measures whenever there is a reason to believe that an individual—whether account-based or walk-in—is intentionally structuring transactions into multiple installments below ₹50,000 to circumvent prescribed thresholds. Such instances shall be treated as potentially suspicious and addressed in accordance with applicable regulatory guidelines.

7. CUSTOMER ACCEPTANCE POLICY

The Company shall follow the following norms while accepting and dealing with its customers:

- No account is opened in anonymous or fictitious/benami name.
- No account is opened where the Company is unable to apply appropriate CDD (Customer Due Diligence) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- No transaction or account based relationship is undertaken without following the CDD procedure.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
- The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a Company desires to open another account with the same Company, there shall be no need for a fresh CDD exercise.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority
- Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

- The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose.
- The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

8. RESPONSIBILITY ALLOCATION

Senior management shall be explicitly responsible for the allocation of these KYC responsibilities, ensuring that the front-line staff are equipped for initial customer identification and verification, the compliance department is empowered for policy oversight, risk assessment, and reporting, and that overall strategic direction is maintained. Specific roles and their corresponding duties in customer due diligence, ongoing monitoring, record-keeping, and reporting of suspicious transactions must be explicitly defined. Regular training programs are essential to ensure all employees understand their KYC obligations and are equipped to identify and report potential risks effectively, thereby fostering a robust anti-money laundering (AML) framework within the Company.

9. CUSTOMER IDENTIFICATION PROCEDURE

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business 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.

The customer identification will be through an introductory reference from an existing customer with a satisfactorily conducted loan account or a person known to us and on the basis of documents provided by the customer or through staff members knowing the potential customer or any other document for identification and proof of residence.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of

its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer. The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements

10. CUSTOMER EDUCATION:

The Company takes adequate measures to educate the customer on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the customers. Wherever we desire to collect any information about the customer for the purpose other than KYC requirement, it will not form part of the loan application. Such information is being collected separately, purely on a voluntary basis in a form prescribed by Company after explaining the objective to the customer and taking the customer's express approval for the specific uses to which such information could be put.

The front desk staffs are specially trained to handle such situations while dealing with customers. The Company takes care to see that implementation of the KYC guidelines in respect of customer acceptance, identification etc. do not result in denial of opening of new loan accounts to general public.

11. MONITORING OF TRANSACTION:

On-going monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts have to be subjected to intensified monitoring. The Company shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

Illustrative list of activities which is construed as suspicious transactions

- Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
    a. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

b. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.

c. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

- Certain Employees of the Company arousing suspicion
  a. An employee whose lavish lifestyle cannot be supported by his or her salary.
  b. Negligence of employees/wilful blindness is reported repeatedly.

- Some examples of suspicious activities/transactions to be monitored by the operating staff:
  a. Multiple accounts under the same name
  b. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc;
  c. There are reasonable doubts over the real beneficiary of the loan
  d. Frequent requests for change of address

12. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT:

As per Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on June 12, 2025), the KYC policy of the company includes the amendment with regard to Money Laundering and Terrorist Financing Risk Assessment by the Regulated Entities (REs).

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

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

b. The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board of the RE, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

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

13. RISK MANAGEMENT

- The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

- Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures.

- As a general rule, the compliance function also provides an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements.

- Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

- The compliance in this regard is put up before the Committee, if any, of the Board on quarterly intervals.

Risk Categorization:

The Company has a system in place for periodical updation of customer identification data after the account is opened. **The periodicity of such updation is not less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.**

All the customers under different product categories are categorized into **low, medium and high risk based on their profile.** The **Credit manager** while appraising the transaction and rendering his/her approval prepares the profile of the customer based on risk categorization. Based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc. Where the credit head believes that a particular customer falling under a category mentioned below is in his judgment falling in a different category, he may categorize the customer, so long as appropriate justification is provided in the customer file.

Indicative List of Risk Categorization:

Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile is categorized as low risk. (In all probabilities the Company is doing and will continue to do their business with such category of customers)

For example: People belonging to lower economic strata of the society whose accounts show small balances and low turnover

i. Government Employee.
ii. Salaried Employees having salary in bank accounts.

Medium Risk Category

a. Salaried employees receiving in salary in cash.
b. Persons in business/industry or trading activity where the area of his residence or place, of business has a scope or history of unlawful trading/business activity.
c. Trusts, charities, etc.
d. Private Ltd companies.

High Risk Category

Customers who are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples are:
1. Non Resident customers
2. High Net worth Individuals
3. Trust, charities, NGO's and Organization receiving donations
4. Companies having close family shareholding or beneficial ownership
5. Firms with 'sleeping partners'
6. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
7. Non face-to-face customers
8. Those with dubious reputation as per public information available
9. Accounts of bullion dealers and jewellers
10. Lawyers
11. Policeman

14. CUSTOMER DUE DILIGENCE PROCEDURE:

I. IDENTIFICATION:

The company shall obtain the following information from an individual while establishing an account based relationship with:

A. Individual

1. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication

2. Permanent Account Number (PAN)
3. Passport
4. Voter's Identity Card
5. Driving License
6. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company.

The KYC Identifier shall only download records from Central KYC Records Registry with an explicit consent to do the same.

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.

B. Proprietary Firms

Any Two of the following documents or the equivalent e-documents shall be obtained:

1. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication)
2. Permanent Account Number (PAN)
3. Registration Certificate including Udyam Registration Certificate (URC) issued by the Government.
4. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
5. Sales and income tax returns.
6. CST/VAT/ GST certificate (provisional/final).
7. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
8. IEC (Import Export Code) issued by office of DGFT
9. 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.
10. Utility bills such as electricity, water, and landline telephone bills
11. Telephone/Fax number/E-mail ID;
12. Recent Color photograph

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

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

C. Company

Each of the following documents or equivalent e-documents shall be obtained:

1. Certificate of incorporation
2. Memorandum and Articles of Association.
3. PAN of the Company.
4. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
5. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
6. The names of relevant persons holding senior management position.
7. The registered office and the principal place of its business, if it is different.

D. Partnership Firms

1. Registration certificate
2. Partnership deed
3. PAN of the firm
4. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5. Names of all the partners
6. Address of the registered office and its principal place of its business, if it is different

E. Trust

Each of the following documents or equivalent e-documents shall be obtained:

1. Registration certificate
2. Trust deed.
3. PAN or Form No. 60 of the trust
4. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5. The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust.
6. The address of the registered office of the trust
7. List of trustees and documents i.e. Aadhaar Card and PAN Card for those who is discharging the role of trustee and authorised to act on behalf of the trust.

F. Unincorporated association or body of individuals

Each of the following documents or equivalent e-documents shall be obtained:

1. Resolution of the managing body of such association or body of individuals.
2. PAN or Form No. 60 of the Unincorporated association or body of individuals
3. Power of attorney granted to him to transact on its behalf.
4. An officially valid document i.e. Aadhar Card and PAN in respect of the person holding an attorney to transact on its behalf.

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

The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above

1. The Credit Head of Company has the power to approve the following document in lieu of ID and address proof

   - A certificate from the public authority (i.e) Gazette Officer of State or Central Govt.,/Magistrate/MRO/VRO/Gram Panchayat Sarpanch/notary public.

In lieu of Identity proof

- Notarized copy of Marriage certificate with the applicant photograph.

In lieu of address proof

- Rental agreement along with rent receipt and utility bill of the Landlord.
- In case the customer has a temporary address being a transit arrangement provided by real estate builder – Allotment letter issued by the builder plus permanent address proof
- In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by Close Relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address.

2. The Credit Head of Company jointly with the concerned Sales Head has further delegated the approval powers to accept the above documents to credit managers, as they may deem fit and necessary, in this regard.

3. In the event of any genuine reason for non-availability of any of the prescribed documents or to approve any deviations for change in the documents prescribed under this policy, the Credit Head jointly with the Sales Head considers approving any other document not stated above based on the product, market requirements and also on the merits of the case.

II. VERIFICATION

As part of the Credit Policy of the Company, documents and implemented appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents or non-documentary verification methods that are appropriate and the associated risks.

i Verification through documents:

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers by the Company as provided in

annexure to this policy. These are appropriately covered in the Credit Policy of the Company.

The Company also accepts physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post is also accepted as an 'Officially Valid Document'.
As per RBI instruction the Company also downloads e-Aadhaar from UIDAI website as an officially valid document subject to the following:

a) If the prospective customer knows only his / her Aadhaar number, the Company needs to print the prospective customer's e-Aadhaar letter in the company directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.

b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the Company prints the prospective customer's e-Aadhaar letter directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.

ii Verification through non-documentary methods:

Indeed the Company mainly depend upon this method:

1. Contacting or visiting a customer;
2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
3. Checking references with other financial institutions; or
4. Obtaining a financial statement.

iii Additional verification procedures.

The business process verification procedures of the Company also address the following situations where:

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The sales executive is not familiar with the documents presented;
3. Where the sales executive is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and
4. If the sales executive cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

The Credit Head along with Sales Head, advise the credit managers to make a personal visit to entangle the situation. The Company will not do any transactions with non-face-to-face customers.

RECORD KEEPING

a. Maintenance of records of transactions:

The Company shall maintain proper record of the transactions as required under Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) read with Rules 3 of the PML Rules as mentioned below:

i. All cash transactions of the value of more than Rs. 2 lacs, though by policy the Company does not accept cash deposits in foreign currency.
ii. All series of cash transactions integrally connected to each other which have been valued below Rs. 2 lacs where such series of transactions have taken place within a month.
iii. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.
iv. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions;
v. Records pertaining to identification of the customer and his/her address; and (vi) All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure III

b. Records to contain the specified information:

The Records referred to above in Rule 3 of PMLA Rules to 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.

c. Maintenance and preservation of records

The company has a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. The company will maintain for at least five years from the date of cessation of transaction between the company and the customer, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

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

15. ENHANCED DUE DILIGENCE

The company is primarily engaged in Loan Against Property (LAP) Business. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing credit policies of the company in respect of its various products ensure that the company is not transacting with such high risk customers.

The company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. The company has established appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the company.

The following are the indicative list where the risk perception of a customer which is considered higher:

i Customers requesting for frequent change of address/contact details
ii Sudden change in the loan account activity of the customers
iii Frequent closure and opening of loan accounts by the customers

Procedure:

a.) Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):

Company shall ensure that the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face-to-face customers.

b.) **Accounts of Politically Exposed Persons (PEPs)**

A. REs shall have the option of establishing a relationship with PEPs provided that:

- sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- the identity of the person shall have been verified before accepting the PEP as a customer;
- the decision to open an account for a PEP is taken at a senior level in accordance with the REs' Customer Acceptance Policy;
- all such accounts are subjected to enhanced monitoring on an on-going basis;
- in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

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

These instructions shall also be applicable to accounts where a PEP is the beneficial owner

CIP Notice:
Enhanced due diligence is in the nature of keeping the account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which forms part of the credit policies of the businesses.

The Company shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

Existing Customer:

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

Reliance on third party due diligence:
The company shall not rely on third party due diligence.

c.) Accounts of non-face-to-face customers (Aadhaar OTP based on-boarding):

- There must be a specific consent from the customer for authentication through OTP.
- Borrowal Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification made through Aadhar Number, Permanent Account Number and such other documents as may be required or as per V-CIP is carried out. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- 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, Company 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.

16. CONFIDENTIALITY OF RISK CATEGORISATION OF CUSTOMER

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

17. PERIODIC REVIEW OF RISK CATEGORISATION OF ACCOUNTS

Periodic review of risk categorisation of accounts, with such periodicity being at least once in six months will be there.

18. AADHAR MASKING

In accordance with applicable regulations and to safeguard the privacy of individuals, the Company shall ensure that Aadhaar numbers collected as part of the Know Your Customer (KYC) process are appropriately masked or redacted in all physical and digital records, wherever such data is stored, processed, or shared. Only the last four digits of the Aadhaar number shall be visible, and all other digits shall be blacked out or otherwise rendered unreadable.

19. ON-GOING DUE DILIGENCE

i. REs shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

ii. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
b. Transactions which exceed the thresholds prescribed for specific categories of accounts.
c. High account turnover inconsistent with the size of the balance maintained.
d. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

iii. The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

Updation/ Periodic Updation of KYC

The Company has adopted a risk-based approach for periodic updation of KYC. However, periodic updation shall be **carried out by the operations team of the Company** 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.

a) **Individuals: (**i.) **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with

the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), letter, etc.

(ii.) **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (if any) (such as online banking / internet banking, mobile application of RE), 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 its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation.

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

iv. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of *updation / periodic updation of KYC* through Aadhaar OTP based e-KYC in non-face to face mode.

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

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

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

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

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the RE are not as per the current CDD standards. Further, in case the validity

of the CDD documents available with the RE has expired at the time of periodic updation of KYC, RE shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

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

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

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

v. REs 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 REs 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 RE 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 REs or any committee of the Board to which power has been delegated.

d) The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the REs the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at REs' end. 96REs

20. APPOINTMENT OF DESIGNATED DIRECTOR / PRINCIPAL OFFICER

The Board of Directors shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. 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". The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

Designated Director

Mr. Rajev Adlakha, Director will be the Designated Director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Principal Officer

Mr. Rajesh Katoch, Director & CEO is designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

As per the RBI guidelines, the Principal Officer is located at our registered office and is responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He maintains a close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

21. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA

In accordance with the requirements under PMLA, the Principal Officer of 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

22. REGISTRATION OF CUSTOMERS ON DARPAN PORTAL IN CASE CUSTOMERS ARE NON-PROFIT ORGANISATIONS

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the RE has ended or the account has been closed, whichever is later.

23. QUARTERLY REPORTING TO BOARD

The Board of Directors shall receive comprehensive quarterly reports detailing the institution's Know Your Customer (KYC) compliance efforts and the overall health of its anti-money laundering (AML) framework.

24. GENERAL

a. Closure of Accounts/Termination of Financing/Business Relationship 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 shall terminate

Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of the key managerial persons authorized for the purpose.

b. KYC for the Existing Accounts: While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions with existing customers would be continuously monitored for any unusual pattern in the operation of the accounts.

c. Updation in KYC Policy of Company: Principal Officer after taking the due approval from the Board of Directors of the Company shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

25. REVIEW

The policy may be amended from time to time by the Board of Directors, but no less than once every year.