



**Know Your Customer  
&  
Anti-Money Laundering Policy  
(KYC and AML Policy)**

**Laxmi India Finance Limited**  
(Formerly known as Laxmi India Finance Private Limited)  
(Formerly known as Laxmi India Finleasecap Private Limited)

**(Sapne Dekho, Bade Dekho, Hamare Saath Unhe  
Pura Hote Dekho)**



<b>Version History</b>		
<b>Version</b>	<b>Name of Policy/Document</b>	<b>Date of Approval/Review</b>
1.0	Know Your Customer & Anti-Money Laundering Policy	July 31, 2015
2.0	Know Your Customer & Anti-Money Laundering Policy	May 06, 2023
3.0	Know Your Customer & Anti-Money Laundering Policy	May 04, 2024
4.0	Know Your Customer & Anti-Money Laundering Policy	August 07, 2024
5.0	Know Your Customer & Anti-Money Laundering Policy	November 13,2024



## 1. Introduction

Laxmi India Finance Limited (Formerly known as Laxmi India Finance Private Limited) (Formerly known as Laxmi India Finleaseap Private Limited) (hereinafter referred as “the Company” or “LIFL” or “Laxmi India”) a Non-Banking Financial Company (‘NBFC’) holding a valid Certificate of Registration (“CoR”) with Reserve Bank of India (‘RBI’) vide registration no. B-10.00318 dated March 31, 2023, classified as NBFC - Investment and Credit Company (NBFC-ICC) under NBFCs-Middle Layer (NBFCs-ML) as per Master Direction- Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, with more than 20 years of experience in asset finance business.

It is focused on offering financing of MSME, Loan against property, commercial vehicles (HCV, LCV, MUV, SUV), Tractors, Two-wheelers, Personal and Business Loan.

## 2. Preamble

RBI advised NBFCs to ensure that a proper policy framework on ‘Know Your Customer’ and Anti-Money Laundering measures with the approval of the Board is formulated and put in place. Accordingly, LIFL has in place Board approved Anti Money Laundering Policy and KYC Norms (the Policy). Based on the experience gained over the past years, the Policy is proposed to be reviewed and improved keeping in view the Master Directions/Circulars on the subject issued by RBI vide **Master Direction - Know Your Customer (KYC) Direction, 2016 vide Master Direction No. RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 and Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under PMLA, 2002 vide Master Circular Number RBI/2015-16/108 DNBR (PD) CC No. 051/03.10.119/2015-16 dated July 1, 2015**, as amended from time to time, (‘RBI’s Guidelines’) which is to be read along with the extant Directions issued by the RBI in this regard or any other applicable law in force. This policy document is a consolidation of various guidelines issued by Reserve Bank of India as also our Company for proper identification of an account holder/customer.

## 3. Objectives, Scope of the Policy

The objective of RBI guidelines is to prevent the company from being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

The company should take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedure and to comply with applicable laws and regulatory guidelines. This policy is applicable to all branches and all other offices of the Company as situated.

## 4. Definitions

- ✚ “**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.
- ✚ "**Aadhaar number**" and “**Authentication**” means an identification number and identification process as defined under sub section (a) and (c) of Section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act' as amended from



time to time, including any statutory modification(s) or re-enactment(s) thereof, for the time being in force;

✚ **“Beneficial Owner” (‘BO’)** to be considered as such BOs in relation to a customer is given below: -

- 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 shareholder’s 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 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 of/entitlement to **more than 10 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.

**Exemption from identification of BO:** The exemption from BO identification has been aligned with that provided in the PML Rules, 2005, such that where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such an entity.

✚ **“Customer”** means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

✚ **“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.

✚ **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and the beneficial owner. Further, the company may obtain KYC Identifier with explicit customer consent to download KYC records from CKYCR, for the purpose of CDD.

✚ **“Customer identification”** means undertaking the process of CDD.



- ✚ **“Designated Director”** means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.
- ✚ **“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.
- ✚ **“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).
- ✚ **“Domestic and cross-border wire transfer”**: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator bank’ or ‘beneficiary bank’ is located in different countries such a transaction is cross-border wire transfer
- ✚ **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
- ✚ **“FATCA”** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S Tax payers or foreign entities in which U.S Tax payers hold a substantial ownership interest.
- ✚ **“Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- ✚ **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- ✚ **Non-profit organisations” (NPO)** means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), 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 (18 of 2013).
- ✚ **“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 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;



- ✚ **“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. For ongoing due diligence, company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.
- ✚ **“Offline verification”** Means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations.
- ✚ **“Principal Officer”** means an officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- ✚ **“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.
- ✚ **“Politically Exposed Persons” (PEPs)** are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc
- ✚ **"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),
  - g. and any agency, office or branch owned or controlled by any of the above persons (a to f)
- ✚ **“Reporting Entity” “REs”** for the purpose of this Policy would mean the Company, Laxmi India Finance Limited (Formerly known as Laxmi India Finance Private Limited) (Formerly known as Laxmi India Finleasecap Private Limited).
- ✚ **“Senior Management”** shall include Designated Director, Principal Officer, Key Managerial Personnel, Compliance Officer and National/Functional Heads of the Company.
- ✚ **"Suspicious Transaction"** means defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
  - a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
  - b. appears to be made in circumstances of unusual or unjustified complexity; or
  - c. appears to not have economic rationale or bona-fide purpose; or
  - d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

**Explanation:**

Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

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

✚ **“Video based Customer Identification Process (V-CIP)”**: an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

✚ **“Wire transfer” related definitions**: related definitions: for purpose of this policy, wire transfer and its related definitions would have the same meaning as assigned to it under the RBI’s Guidelines on the Know Your customer and Anti-Money Laundering Measures, as amended from time to time.

## 5. Money Laundering and Terrorist Financing Risk Assessment

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

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

- b. The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the Company, in alignment with the outcome of the risk assessment exercise. However, it shall be reviewed 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. The Company 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, The Company shall monitor the implementation of the controls and enhance them if necessary.

## 6. KYC Standards

The Company hereunder framing its KYC policies incorporating the following four key elements:

- (i) **Customer Acceptance Policy (CAP);**
- (ii) **Risk Management**
- (iii) **Customer Identification Procedures;**
- (iv) **Monitoring of Transactions;**



### (i) Customer Acceptance Policy (CAP)

- (a) No account is opened in anonymous or fictitious/benami name.
- (b) No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- (c) No transaction or account-based relationship is undertaken without following the CDD procedure.
- (d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- (e) Additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer.
- (f) REs shall apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.
- (g) CDD Procedure is followed for all the joint account holders, while opening a joint account.
- (h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- (i) 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 indicated in Chapter IX of the **Master Direction - Know Your Customer (KYC) Direction, 2016**.
- (j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- (k) 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).
- (l) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

### (ii) Risk Management

- (a) The Board of Directors of LIFL has ensured that an effective KYC program is in place and has established appropriate procedures and is overseeing its effective implementation. The program covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has been explicitly allocated to ensure that LIFL's policies and procedures are implemented effectively.
- (b) Customers shall be categorised as low, medium and high-risk category, based on the assessment and risk perception of the RE.
- (c) Broad principles may be laid down by the REs for risk-categorisation of customers.
- (d) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- (e) 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.
- (f) LIFL has already ensured that the Sales, Operational and Credit staff are aware that no loan accounts will be created unless the KYC procedures are adhered to completely.
- (g) Examples of customers requiring Lower due diligence may include: -
  - i. Salaried employees with well-defined salary structures;



- ii. People working with government owned companies, regulators and statutory bodies, etc;
- iii. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
- iv. People working with Public Sector Units;
- v. People working with reputed Public Limited Companies and Multinational Companies

(h) Examples of customers requiring medium due diligence may include: -

- i. Salaried applicant with variable income/ unstructured income receiving Salary in cheque;
- ii. Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialling (IDD) call service.
- iii. Companies having close family shareholding or beneficial ownership

(i) Examples of customers requiring higher due diligence may include: -

- i. non-resident customers,
- ii. high net worth individuals,
- iii. trusts, charities, NGOs and organizations receiving donations,
- iv. firms with 'sleeping partners',
- v. politically exposed persons (PEPs) of foreign origin,
- vi. non-face to face customers, and
- vii. those with dubious reputation as per public information available, etc.
- viii. Individuals and entities listed or identified in – various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267, schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.
- ix. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.
- x. Gambling/gaming including “junket operators” arranging gambling tours.
- xi. Jewellers and Bullion Dealers

(j) Adoption of customer acceptance policy and its implementation shall not become too restrictive and the Company will strive not to inconvenience the general public, especially those who are financially or socially disadvantaged.

### **(iii) Customer Identification Procedure (CIP)**

REs shall undertake identification of customers in the following cases:

- (a) Commencement of an account-based relationship with the customer.
- (b) Carrying out any international money transfer operations for a person who is not an account holder of the RE.
- (c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- (d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
- (e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- (f) When a RE has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- (g) REs shall ensure that introduction is not to be sought while opening accounts.

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



- (a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
- (b) Adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- (c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- (d) The third party shall not be based in a country or jurisdiction assessed as high risk.
- (e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

The Company will obtain the documents as per the nature of customers which are as mentioned below:

➤ **Accounts of Individuals**

In case of customers that are natural person the Company will obtain sufficient identification data to verify (a) the identity of customer (b) his/her address/ location and (c) his/her recent photograph. The Company may also undertake V-CIP to carry out CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, and shall adhere to the standards as prescribed under PML Act/ RBI guidelines/KYC Policy. The true identity and bonafides of the existing customers and new potential customers opening credit accounts with the Company and obtaining basic background information would be of paramount importance.

➤ **Other than individual accounts**

For customers that are legal person or entities the Company will (a) verify the legal status of the legal person/entity through proper and relevant documents, (b) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (c) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. The Company may also undertake V-CIP to carry out CDD in case of new customer on-boarding for authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers and shall adhere to the standards as prescribed under PML Act/ RBI guidelines/KYC Policy.

➤ **Accounts of companies and firms**

Branches need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with the company. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.

➤ **Accounts of Politically Exposed Persons (PEPs) resident outside India**

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The branches should seek prior approval of their concerned Credit Heads for opening an account in the name of PEP.

➤ **Accounts of proprietary concerns**



The Company may undertake V-CIP to carry out CDD of a proprietorship firm, by obtaining the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 of Master Direction, apart from undertaking CDD of the proprietor and shall adhere to the standards as prescribed under PML Act/ RBI guidelines/KYC Policy. The Company should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. the Company may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the 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 and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns. The company shall take the “Registration certificate” as a proof of business/ activity in the name of the proprietary firm includes “Udyam Registration Certificate (URC) issued by the Government”.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

➤ **Obtaining Guarantor on credit facilities**

The Company generally insists on “Guarantee” by a known person (who becomes guarantor to a particular credit facility). Obtaining Guarantee from a known person is a process of ascertaining the identity of a person and his acceptability for establishing business relationship and verifying the true identity of the intending customer before opening a credit account. Further, Guarantor also acts as an introducer of the customer to the Company for the credit facilities.

➤ **Liabilities of the Guarantor**

Guarantor is legally responsible to the Company for the repayment of the credit facilities by the customer and is expected to be in a position to identify/trace the account holder in case of need.

➤ **Procedure for providing Guarantee**

The Guarantor will be required to sign on the agreement entered into with the Customer at various places provided in the loan agreement form.

The Guarantor will be normally required to visit the Company’s branch for signing the agreement. However, this need not be compulsory.



➤ **Closure of accounts**

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 will consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions will be taken at a reasonably senior level.

**(iv) Monitoring of Transactions**

(i) Ongoing monitoring is an essential element of effective KYC procedures. LIFL can effectively control and reduce risk by having an understanding of the normal and reasonable activity of the customers. However, the extent of monitoring will depend on the risk sensitivity of the account. Since LIFL being a Non Deposit Accepting NBFC will not have any deposit accounts, this situation will hardly arise, but LIFL will in any case pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. For ongoing due diligence, REs may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

(ii) LIFL will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. LIFL will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002 (and the Amended Act, 2009). It will also ensure that transactions of suspicious nature and/or any other type of transaction notified under section 12 of the PML Act, 2002 (and the Amended Act, 2009), is reported to the appropriate law enforcement authority.

A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

REs shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out 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. Policy in this regard shall be documented as part of REs' internal KYC policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated.

<b>A. INDIVIDUAL CUSTOMERS</b>	
a) No change in 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 Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.
b) Change in address	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 (such as online banking / internet banking, mobile application of Company), letter etc. The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.
c) Accounts of customers who were minor at the time of opening account on their becoming major	A fresh photograph shall be obtained from the customer on their becoming a major and it shall be ensured that CDD documents as per the current CDD standards are available with the Company. The Company may also carry out fresh KYC of such customers, wherever required.



<p>d) Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode</p>	<p>Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall, however, 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.</p>
<p><b>B. CUSTOMERS OTHER THAN INDIVIDUALS (LEGAL ENTITY)</b></p>	
<p>a) No change in KYC information</p> <p>b) Change in KYC information</p>	<p>A self-declaration shall be obtained from the Legal Entity (LE) customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. The Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.</p> <p>The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.</p>
<p><b>ADDITIONAL MEASURES</b></p>	<p>a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.</p> <p>b) Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.</p> <p>c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.</p> <p>d) In order to ensure customer convenience, Company 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 Company or any committee of the Board to which power has been delegated.</p> <p>e) Company shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.</p>
<p><b>OBLIGATIONS OF CUSTOMERS</b></p>	<p>The customers are required to submit the updated KYC Documents to the company, 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 company 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 company's end.</p>

**Enhanced due diligence (non-face to face customer onboarding)**



The Company need to apply enhanced due diligence measures in case of customers onboarding through non-face-to-face method. Presently, the Company onboard the customers through physical verification and it shall comply with the respective provisions of RBI KYC & AML Master Direction as and when Company starts the procedure of onboarding the customers through non- face-to-face mode or V-CIP.

#### **7. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)**

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.

#### **8. Appointment of Designated Director**

Mr. Deepak Baid shall be appointed & designated as "Designated Director" to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and rules.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

#### **9. Wire Transfer**

Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. The Company shall follow the responsibilities, procedure and other obligations applicable to the Company laid down in the rules for wire transfer occurring either domestic or cross- border of RBI KYC & AML Master Direction.

#### **10. Appointment of Principal Officer**

Mr. Sourabh Mishra has nominated as Principal Officer of the Company, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under PML Act/ KYC Policy.

The name, designation and address of the Principal Officer shall be communicated to the FIU-IND. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

#### **11. Compliance of KYC policy:**

a) LIFL to ensure compliance with KYC Policy through:

- (i) The functional heads of the company will constitute as 'Senior Management' for the purpose of KYC compliance.
- (ii) Allocation of responsibility for effective implementation of policies and procedures at HO / Regional Office/ Zonal Office / Branch Office level.
- (iii) All HO Departments to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
- (iv) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements.



- (v) Internal auditor shall verify the compliance with KYC / AML policies and procedures and submit audit notes and compliance to the Audit Committee on periodic basis.
- b) The company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

## **12. Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)**

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking/Financial companies in regard to preservation and reporting of customer account information.

LIFL has a system of maintaining proper record of transactions as required under Prevention of Money-Laundering Act and value of transactions, the procedure and manner of maintaining and verification.

### **(i) Maintenance of records of transactions:**

The company shall maintain the proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

- a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh or its equivalent in foreign currency;
- c) all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency;
- d) 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 transaction;
- e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- f) all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
- g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

### **(ii) Information to be preserved:**

The company will maintain all necessary information in respect of transactions referred to in Rule 3 to permit reconstruction of individual transaction, including 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.

### **(iii) Maintenance and Preservation of Records**



LIFL has an appropriate 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 necessary records of transactions, both domestic or international which permits 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 are maintained for at least five years from the date of cessation of transaction between the LIFL and the client.

All the records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the 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 are made available to the competent authorities upon request.

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. If such customers are not registered, the company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the the Company has ended or the account has been closed, whichever is later.

**(iv) Reporting to Financial Intelligence Unit – India: -**

There are following below mentioned reporting which are filed with FIU-ID at FINGATE:

Snapshot of various Transactions Reporting Formats to Financial Intelligence Unit India					
Sl.	Report	Description	Amount	Frequency and Due Date	Formats
1	<b>Cash Transaction Reports (CTR)</b>	All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency. All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month	Rs. 10,00,000/-	Event Based and 15th day of the succeeding month	As Prescribed from time to time.
2	<b>Counterfeit Currency Reports (CCR)</b>	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions			
3	<b>Non-Profit Organization Transaction Report (NTR)</b>	All transactions involving receipts by non-profit organizations of value more than Rs. Ten lakhs or, its equivalent in foreign currency			
4	<b>Cross Border Wire Transfer Reports (CBWTR)</b>	All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.	Rs. 5,00,000/-		



5	<b>Report on sale/purchase of immovable property (IPR)</b>	All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity*, as the case may be.	Rs. 50,00,000/-	Event Based and 15th day of the month succeeding the quarter.	
6	<b>Suspicious Transaction Reports (STR)</b>	All suspicious transactions whether or not made in cash		Event Based and Not later than seven working days on being satisfied that the transaction is suspicious.	
<b>In terms of the PMLA rules, the Company will report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address and portal</b>					
<i>Address</i>			<i>Portal</i>		
<i>Director, FIU-IND, Financial Intelligence Unit-India, 6<sup>th</sup> Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021</i>			<i><a href="http://fiuindia.gov.in/">http://fiuindia.gov.in/</a></i>		

### 13. Combating financing of terrorism

In terms of PMLA Rules, suspicious transaction shall include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. The company shall, before opening any new account, ensure that the name/s of the proposed customer does not appear in the list. Further, the company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the company as an integral part of recruitment/hiring process of personnel.

### 14. Filing of Suspicious Transaction Report (STR)

LIFL should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. It was clarified that in the circumstances when a NBFC believes that it would no longer be satisfied that it knows the true identity of the account holder, the Company should also file an STR with FIU-IND.



## **15. Policy Review**

The Board shall review and amend this policy as and when required.

If at any point a conflict of interpretation / information between the policy and any regulations, rules, guidelines, notification, clarifications, circulars, master circulars/ directions issued by relevant authorities (“Regulatory Provisions”) arises, then interpretation of the Regulatory Provisions shall prevail.

In case of any amendment(s) and/or clarification(s) to the Regulatory Provisions, the policy shall stand amended accordingly from the effective date specified as per the Regulatory Provisions.



**Annexure-I**  
**Illustrative Customer identification procedure**

<b>Types of customers: features to be verified.</b>	<b>Illustrative Documents to be obtained</b>
<p>Accounts of individuals:</p> <ul style="list-style-type: none"> <li>- Legal name and any other names used</li> <li>- Correct permanent address</li> </ul>	<p>(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v) Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number (vii) Identity card (subject to the bank's satisfaction) (viii) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (ix) Aadhar Card including e-Aadhar.</p> <p>(i) Telephone bill (ii) Bank account statement (iii) letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Aadhar Card including e-Aadhar (vii) Letter from employer (subject to satisfaction of the Company) (any one document which provides customer information to the satisfaction of the Company will suffice).</p>
<p>Accounts of partnership firms</p> <ul style="list-style-type: none"> <li>• Legal name</li> <li>• Address</li> <li>• Names of all partners and their addresses</li> <li>• Telephone numbers of the firm and partners.</li> </ul>	<p>(i) Registration certificate, if registered (ii) Partnership deed (iii) PAN of the Partnership Firm (iv) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (v) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (vi) Telephone bill in the name of firm/partners (vii) the names of all the partners; and (viii) address of the registered office, and the principal place of its business, if it is different.</p>
<p>Accounts of companies</p> <ul style="list-style-type: none"> <li>• Name of the company</li> <li>• Principal place of business</li> <li>• Mailing address of the company</li> <li>• Telephone/Fax Number.</li> </ul>	<p>(i) Certificate of Incorporation and Memorandum &amp; Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill (vi) the names of the relevant persons holding senior management position; and (vii) the registered office and the principal place of its business, if it is different.</p>
<p>Accounts of trusts &amp; foundations</p> <ul style="list-style-type: none"> <li>• Names of trustees, settlers, beneficiaries and signatories.</li> <li>• Names and addresses of the founder, the managers/ directors and the beneficiaries. Telephone/fax numbers</li> </ul>	<p>(i) Certificate of registration, if registered (ii) Trust Deed (iii) PAN or Form 60 of the Trust (iv) Power of Attorney granted to transact business on its behalf (v) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses. (vi) Resolution of the managing body of the foundation/Association. (vii) Telephone bill.</p>



<ul style="list-style-type: none"> <li>Telephone/fax numbers.</li> </ul>	<p>(vi) the names of the beneficiaries, trustees, settlor and authors of the trust (vii) the address of the registered office of the trust; and (viii) list of trustees and documents, as specified in Section 16, for those discharging role as trustee and authorised to transact on behalf of the trust.</p>
<p>Accounts of Proprietorship Concerns</p> <ul style="list-style-type: none"> <li>Proof of the name, address and activity of the concern</li> </ul>	<p>(i) Registration certificate (in the case of a registered concern)</p> <p>(ii) Certificate/license issued by the Municipal authorities under Shop &amp; Establishment Act,</p> <p>(iii) Sales and income tax returns</p> <p>(iv) CST/VAT certificate/GST Certificate</p> <p>(v) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities</p> <p>(vi) Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department, etc. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of the bank account etc.</p> <p>(vii) The 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.</p> <p>(viii) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.</p> <p>Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.</p>