



For	Ladderup Finance Limited
Content	Know Your Customer and Anti-Money Laundering Policy
Version	1.0
Date of Review/ Revision	7th February 2025

1. BACKGROUND

- Reserve Bank of India (hereinafter 'RBI'), one of the regulatory agencies entrusted with the responsibility of driving the anti-money laundering initiatives, has advised NBFCs to follow certain customer identification procedures for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting them to the appropriate authorities. RBI revisits these guidelines from time to time keeping in view the recommendations of Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT).
- RBI advises 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, Ladderup Finance Limited ('Company') has put in place a Know Your Customer (KYC) & Anti Money Laundering Policy with the approval of the Board in compliance with requirement of the Master Directions titled 'Know Your Customer (KYC) Directions, 2016' issued by the RBI dated 25th February, 2016 ('Master Directions').
- The intent of the policy is to know and understand the Company's customers and their financial dealings better which in turn shall help in managing the risks prudently and prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities.

As per the aforementioned Master Directions, the policy has the following four key elements:

- Customer Acceptance Policy;
- Risk management;
- Customer Identification Procedures (CIP); and
- Monitoring of Transactions.

2. POLICY OUTLINE:

- **Specifying the 'Senior Management' for the purpose of KYC Compliance:**

The Board has identified Company Secretary who shall be responsible for ensuring the KYC compliance.

- **Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures:**

The Board or any other committee to whom the power has been delegated by the Board shall carry out concurrent/ internal audit on a quarterly basis, to verify the compliance with this Policy and procedures laid herein.

- **Submission of quarterly audit notes and compliance:**

The aforesaid audit report shall thereafter be submitted to the Board of Directors or Audit Committee for their review and comments.

3. CUSTOMER ACCEPTANCE POLICY:

For the purpose of this policy, a “Customer” means any person, as defined in the RBI’s Master Directions on ‘Know Your Customer’ and Anti-Money Laundering Measures, as amended from time to time. For the purpose of clarification, it may be noted that “Customer” means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

A “beneficial owner” (‘BO’) in relation to a Customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered into with the Company.

The guidelines for Customer Acceptance Policy (CAP) for the Company are as given below:

- The Company shall not open any account on fictitious/ benami name(s).
- The Company shall have in place a standard customer identification procedure (specified in Para 5 below) and the same should be adhered to before opening an account.
- The Company shall not open an account in cases where it is unable to carry out appropriate Customer Due Diligence (CDD) measures due to non-cooperation by the customer or non-reliability of the documents/ information furnished by him/her. CDD means identifying and verifying the Customer and the BO using ‘Officially Valid Documents’ (OVD) as a ‘proof of identity’ and a ‘proof of address’. Here, OVD means any one of the six OVDs submitted by the Customer, as mentioned herein below:
 - the Passport,
 - the Driving License,
 - Proof of possession of Aadhaar number,
 - the Voter's Identity Card issued by the Election Commission of India,
 - the job card issued by NREGA duly signed by an officer of the State Government,
 - letter issued by the National Population Register containing details of name and address.
- The Customer shall mandatorily submit:
 - a. a copy of Permanent account number (PAN) card or Form No. 60 as defined in Income-tax Rules, 1962;
 - b. one recent photograph
- The Company shall carry out offline verification of a Customer if he is desirous of undergoing Aadhaar offline verification for identification purpose. Offline verification maybe carried out through the modes recognized by the Unique Identification Authority of India (UIDAI) i.e. using the QR Code or a digitally signed XML.
- While collecting any OVD, the Company shall ensure to obtain the Certified Copy of the OVD. For the purpose of this Policy, ‘Certified copy of OVD’ shall mean Certified Copy of OVD as defined in the KYC Directions. In case of resident individuals, obtaining a certified copy shall mean comparing the copy of officially valid document so produced by the Customer with the original and recording the same on the copy by the authorised officer of the Company.
- The Company shall, where Customer submits his Aadhaar number, ensure such Customer to redact or blackout his Aadhaar number through appropriate means.
- The Company shall not undertake transaction or accounts based relationship without following the CDD procedure.
- The Company shall ensure that documents and other information is obtained from the customer depending on perceived risk and keeping in mind the requirements of

Prevention of Money Laundering (PML) Act, 2002 and guidelines issued by RBI from time to time.

- The Company shall specify the mandatory information to be sought for KYC purpose while opening the account and during the periodic updation.
- The Company shall obtain the explicit consent of the consumer for optional/additional information 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 RE desires to open another account or avail any other product or service from the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
- CDD procedure shall be followed for all co-borrowers while entering into a co-borrowing transaction.
- The Company shall have in place a risk strategy. Each Customer should be classified into the appropriate risk category after considering the background of the Customer, the nature of his business, the location of his business, the locations from where majority of his business, financial / social standing of the Customer, the amount involved in the financial transaction etc. based on risk categorization; containing information on the Customer's identity, nature of business activity.
- In case of proprietorship firms, in addition to the proprietor's ID, the firm's ID (business proof) also would be obtained at least through two documents such as ITR, Import-Export Code/Utility bill/Permit by local authority etc.
- The Company shall ensure that proper profiling is done with respect to the Customers.
- The Company shall ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. For this purpose, the Company shall, among other things, refer the "ISIL (Da'esh) & Al-Qaida Sanctions List"¹ and
- the "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.²
- Further, the CAP shall not result in exclusion of general public, especially the financially and socially disadvantaged.
- Based on the risk categorization, the Company shall undertake following Customer acceptance procedure on a case to case basis:
- Internal dedupe - Checking the internal records of the Company to confirm about any past dealings of the Customer with the Company either as borrower, co-borrower or guarantor;
- External dedupe - Verifying with the database maintained by at least one RBI approved credit information bureau;
- Tele verification with the Customer.

4. CUSTOMER IDENTIFICATION PROCESS:

- Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. This Policy clearly spells out the Customer Identification Procedure to be carried out at the time of establishing an account. The Company is required to ensure that.
 - The authorized representative of the Company shall obtain the KYC documents whenever there is doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
 - The authorized representative, while conducting verification, shall satisfy itself that the address contained in the OVD is the updated or current address of the customer. If the OVD does not contain current address of the customer, a proof of current address such as
-

a utility bill, property tax receipt, pension or family pension payment orders (PPOs) or other documents as mentioned in the KYC directions shall be obtained from the customer, which shall be deemed to be OVD for the purpose of serving as a proof of address.

- Further, the Company shall obtain from the customer, an OVD with current address within three months of submitting the aforementioned documents.
- The authorized representative also would have the process of allotting a Unique Customer Identification Code (UCIC) for easy identification of all the relationships of any customer with the Company.
- Information collected for the purpose of opening an account would be kept as confidential and would not be divulged to outsiders for cross selling or any other purpose other than for the statutory requirement of sharing the customer account
- Details with at least all the Credit Information Companies (CICs) approved by RBI. Information sought from the customer would be relevant to the perceived risk and would not be intrusive.
- For the purpose of verifying the identity of customers and the associated documents/information, the Company, may rely on a third party. However, the ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the company.
- Decision-making functions of determining compliance with KYC norms shall not be outsourced.
- The beneficial owner in the case of trust, partnership and joint stock companies would be reckoned in the manner described in para 3 of this Policy.
- If the OVD submitted by the customer at the time of KYC includes both address and identity proof then he is not required to submit additional OVD.
- In case it is observed that the address mentioned as per 'proof of address' has undergone a change, Company shall ensure that fresh proof of address is obtained within a period of six months.
- Documentation requirements and other information is to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by RBI from time to time.
- The Company shall not start or close a business transaction where the Company is unable to apply appropriate CDD measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company.
- The Company shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Further, an online portal was set up in order to facilitate storage of the KYC documents on a centralized manner which was implemented vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015. In this regard the Company will take necessary steps to upload the KYC documents in the online portal with the Central KYC Registry within three days after the commencement of an account-based relationship with a client.

5. MONITORING OF TRANSACTIONS:

- The Company shall undertake on-going due diligence of customers so as to ensure that the transactions carried out by them are in line with the knowledge available to them about the customer, his risk profile, and the source of funds.

- The extent of monitoring an account shall be aligned with the risk category of the customer.
- The Company shall maintain proper record of all cash transactions of Rs.10 lakh and above and have in place internal monitoring system.
- In case of such unusual transactions that fall outside the regular pattern of activity, the Company shall strive to have an understanding of the normal and reasonable activity of the customer through personal visits and by observing the transactions and conduct of the borrower account.
- The following list of transactions, will be regularly monitored by the Company:
 - 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.

6. REPORTING OF TRANSACTIONS TO FIU-IND:

- The Company will maintain proper record and furnish to the Director, FIU-IND, all transactions/information prescribed in Rule 3 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.
- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency, which if taken together, amount to more than rupees ten lakhs, where such series of transactions have taken place within a month (CTR) shall be reported to FIU-IND within 15th day of the succeeding month.
- All such transactions, as specified in para above, would be reported to and reviewed by Principal Officer who would enquire into the matter and decide whether the transaction would qualify to be termed as a suspicious transaction. When it is believed that we no longer are satisfied that we know the true identity of the account holder, STR would be filed with FIU-IND. The Principal Officer would file the Suspicious Transaction Report with the Director, Financial Intelligence Unit-India (FIU-IND) within 7 days of identifying them. After filing STR, transactions would be allowed to be continued in the account unhindered and the customer would not be tipped in any manner.
- All CTR/STR would be filed electronically or as per the norms stipulated by FIU-IND from time to time. The STR would be filed even for attempted transactions.
- The Company has created a document retention policy which would be reviewed periodically to be in compliance with the requirements of PMLA. The following documents/ records would be held for a period of 10 years:
 - Records with respect to the cash transactions of value of more than Rs. 10 lacs
 - Records with respect to series of cash transactions integrally connected to each other, taken together amounting to more than Rs.10 lacs within a month
 - Records with respect to transactions where counterfeit currency notes have been used
 - Records with respect to all suspicious transactions
 - KYC documents after the business relationship has ended.
 - The documents/ records maintained would hold the following information
 - Nature of the transaction;
 - Amount of the transaction;
 - Date on which the transaction was conducted; and
 - The parties involved in the transaction.

7. CUSTOMER EDUCATION:

Implementation of KYC procedures can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the Company will take necessary steps, as may be required, to educate the customer of the objectives of the KYC programme.

8. APPOINTMENT OF PRINCIPAL OFFICER:

- Chief Financial Officer of the company has been appointed as the Principal Officer in compliance with Rule 2 (f) of the Maintenance of Record Rules of the PMLA.
- The Principal Officer, under the supervision and guidance of the Designated Director, shall be responsible to ensure overall compliance specified under the Act and the Rules/ Regulations thereunder.

The Principal Officer would perform the following duties:

- a. Develop effective AML programs, including training programs
- b. Assist the business in assessing how the system can be abused
- c. Identify suspicious activity
- d. Monitor implementation of this Policy
- e. Submit reports to statutory bodies and management

9. APPOINTMENT OF DESIGNATED DIRECTOR:

Managing Director of the company has been appointed as the Designated Director in compliance with Rule 2 (ba) of the Maintenance of Record Rules of the PMLA. The Designated Director shall be responsible to ensure overall compliance specified under the Act and the Rules / Regulations thereunder.

10. APPOINTMENT OF THIRD PARTY:

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

- The appointment of such third party is in accordance with the outsourcing policy of the Company.
- Necessary information of such customers' due diligence that is carried out by the third party is immediately obtained by the Company.
- Adequate steps are taken by the Company 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.
- 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.

- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

11. PERIODIC UPDATION:

- 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 subject to the following conditions:
 - a. Fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorised as 'low risk', when there is no change in status with respect to their identities and addresses and a self-certification to that effect is obtained.
 - b. A certified copy of the proof of address forwarded by 'low risk' customers through mail/post, etc., in case of change of address shall be acceptable.
 - c. Physical presence of low risk customer at the time of periodic updation shall not be insisted upon.
 - d. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.
 - e. Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

12. AUDIT:

- The Board of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensure their effective implementation;
- Internal audit and compliance function would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of Company's own policies and procedures, including legal and regulatory requirements.
- Concurrent/ Internal Auditors shall 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 would be put up before the Audit Committee of the Board on quarterly basis;
- The Company shall have an on-going employee training programme with different focuses for frontline staff, compliance staff and staff dealing with new customers and educating them with respect to the objectives of the KYC Programme.

13. POLICY REVIEW:

This Policy must be reviewed at least once in a financial year or at such intervals as may be deemed necessary by the Board of Directors.
