

GALADA FINANCE LIMITED

Know Your Customer (KYC) Guidelines & Anti-Money Laundering Standards (AML) Policy

Policy dated 27.05.2025

GLOSSARY

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PMLA	Prevention of Money Laundering Act
KYC	Know Your Customer
AML	Anti-Money Laundering
NBFC	Non-Banking Financial Companies
FIU-IND	Financial Intelligence Unit – India
OVD	Officially Valid Document
CERSAI	Central Registry of Securitization Asset Reconstruction and Security Interest
CDD	Customer Due Diligence
V-CIP	- Video based Customer Identification Process

1. PREAMBLE

The Reserve Bank of India (RBI) had advised all the NBFCs to ensure that a proper policy framework on Know Your Customer and Anti Money Laundering measures is formulated and put in place with approval of the Board. The policy was to lay down the systems and procedures to help control financial frauds, identify money laundering and suspicious transactions, combating financing of terrorism and careful scrutiny/ monitoring of large value of cash transactions. Pursuant to advice from the RBI, a Know Your Customer and Anti Money Laundering Policy (the Policy) was put in place with approval of the Board on May 29, 2014.

Since then, the Policy has been reviewed and revised with the approval of the Board, in line with the notifications on AML KYC issued RBI from time to time.

Presently, the Revised Policy is approved by the Board on May 27, 2025 to comply with the modification effected by RBI to its KYC Master Directions .

2. POLICY OBJECTIVES

The basic objectives of the policy:

- a. To comply with the guidelines issued in Prevention of Money Laundering Act (PMLA), 2002.
- b. To adhere the “Know Your Customer” (KYC) policies and procedures issued by Reserve Bank of India.
- c. To prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities

3. SCOPE

KYC and AML Policy guidelines are applicable to all the functions of the organization dealing with customers, vendors / service providers and employees. Functions should adhere to the guidelines mentioned in this policy while drafting their internal policies, procedures, products etc.

Know Your Customer policy envisages the following key elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)
- Monitoring of transactions
- Risk management

4. Definitions

‘Customer’ is defined to mean 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

“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, 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. The customers should be asked to redact or blackout Aadhaar number and the functions responsible should ensure that same.

“Beneficial owner” is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

“Digital KYC” Capturing live photo of the customer and OVD 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 authorized officer of the Company

“Equivalent e-document” 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. This may be obtained for individuals and also from non-individual customers.

“Video based Customer Identification Process (V-CIP)” A method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for Customer Due Diligence (CDD) purpose, and to ascertain the veracity of the information furnished by the customer. This process is to be treated as face-to-face process for the purpose of this Policy

5. CUSTOMER ACCEPTANCE POLICY

For the Customer Acceptance following criteria should be followed:

- No account should be opened in anonymous or fictitious/benami name(s) and accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed later).
- No account should be 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
- Documentation requirements and other information should be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act 2002 and guidelines issued by Reserve Bank from time to time.

- 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
- No transaction or account-based relationship is undertaken without following the CDD procedure
- 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
- 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 above Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged}

6. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

The organization should identify the customer and verifying his/ her identity by using reliable independent sources of documents, data or information to ensure that the customer is not a fictitious person.

The organization should be able to satisfy the competent authorities that due diligence was observed based on risk profile of the customer in compliance with extant guidelines in place. Besides risk perception, the nature of information / documents required would also depend on the type of customer (individual, corporate etc.)

Identification as under, would be required to be obtained in respect of different classes of customers:

a. Customers that are natural persons:

- Address/location details
- Identity Proof and Recent photograph

b. Customers that are legal persons:

- Legal status of the legal person/entity through proper and relevant documents.
- Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified.
- Understand the ownership and control structure of the customer and determine who are the natural persons and ultimately control the legal person.

Individual Customers (Mandatory Pan Number)

- a. The customers would submit OVD for identity and address.
- b. Individual customers have to mandatorily submit the Permanent Account Number or Form No. 60. This would also apply to individuals who are beneficial owner, authorized signatory or power of attorney holder related to any legal entity.

For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

Proprietorship Firms

Documents which could be obtained as proof of business/activity for proprietary firms (any one or more), in addition to the documents of the proprietor as individual:

- a. Registration Certificate
- b. Certificate/ license issued by the Municipal authorities under Shop & Establishment Act,
- c. Sales and Income tax returns,
- d. GST certificate (Provisional/Final)
- e. IEC (Importer Exporter Code) issued to the proprietary concern by the office of Director General of Foreign Trade (DGFT)/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute
- f. 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
- g. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern

Any one of the above documents in the name of the proprietary concern would be sufficient.

Partnership Firms:

Where the customer is a partnership firm, the certified copies of the following documents should be obtained:

- a. PAN of the partnership firm
- b. Certificate of registration
- c. Partnership deed.
- d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf

- e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf along with any OVD for identity and address proof and one recent photograph of such persons.

Trusts

Where the customer is a trust firm, the certified copies of the following documents should be obtained:

- a. PAN/Form No. 60 of the entity
- b. Certificate of registration
- c. Trust deed.
- d. Power of Attorney granted to a member or an employee of the firm to transact business on its behalf
- e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf
- f. and any OVD for identity and address proof and one recent photograph of such persons

Unincorporated Bodies

Where the customer is an unincorporated association or a body of individuals, the certified copies of the following documents should be obtained:

- a. PAN/Form No. 60 of the entity
- b. Resolution of the managing body of such association or body of individuals;
- c. Power of attorney granted to him to transact on its behalf
- d. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf
- e. and any OVD for identity and address proof and one recent photograph of such persons.

Companies:

Where the customer is a Company, the certified copies of the following documents should be obtained:-

- a. PAN of the Company
- b. Certificate of incorporation
- c. Memorandum and Articles of Association
- d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their Permanent Account Number or Form 60 and any OVD or Aadhaar card for identity and address proof and one recent photograph of such persons

7. Risk Management

Concurrent/Internal Audit

Internal Auditors should have a process to verify the compliance with KYC/AML policies and procedures across the organization including the application of KYC procedures at the branches and comment on the lapses observed. The compliance in this regard should be put before the Audit Committee of the Board on quarterly basis.

Money Laundering (ML) Risk Assessment exercise should be carried out annually to identify, assess and take effective measures to mitigate the money laundering risk arising from clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The risk assessment should be commensurate to size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment should also take cognizance of the overall sector-specific vulnerabilities, if any, that RBI may share time to time.

Risk Based Approach (RBA) should be applied for mitigation and management of risks identified and Board approved policies, controls and procedures in vogue should be accordingly aligned

Training

There is ongoing employee training program so that the staff is adequately trained in KYC procedures.

8. Customer Due Diligence (CDD)

For undertaking CDD, either of the following should be obtained from an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity

- a. Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962
- b. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. 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 the Aadhaar regulations

S.NO	Nature of the Document	Type of Verification
I	Proof of possession of Aadhaar number where offline verification can be carried out	Offline verification
II	Proof of possession of Aadhaar number where offline verification cannot be carried out	Online
III	Any OVD containing the details of identity and address	Online

9. Allotment of UCIC to each of the borrower, borrower wise classification of accounts and Record Retention

For each of the Borrowers the company will issue UCIC (Unique Customer Identification Code) also ensure borrower wise classification of accounts. Records pertaining to identification of the customer and his address obtained while opening his account and during course of business relationship should be preserved for at least eight years after the business relationship has ended.

10. Central KYC Registry (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI)

11. Customer Education

The organization ~~should prepare~~ specific literature / pamphlets etc., to educate the customer of the objectives of the KYC program. The frontline lending and operating managers should be fully equipped with the compliance requirements of KYC guidelines in respect of new customer acquisition and shall adhere to the Customer Identification & Acceptance procedure.

12. Principal Officer and Designated Director

The senior management officer (SVP and above) should be the Principal Officer for KYC/AML matters who will be responsible for implementation of and compliance with this policy. His duties, in this regards, will be as follows:

- Overall monitoring of the implementation of the organization's KYC/AML policy
- Monitoring and reporting of transactions, and sharing of information, as required under the law.
- Maintaining liaison with the law enforcement agencies, banks and other institutions, which are involved in the fight against money laundering
- Ensuring submission of periodical reports to the Top Management /Board

The Managing Director or a whole – time Director should be appointed as the “Designated Director” for ensuring compliance with the obligations under the PMLA, 2002.

13. Review of the Policy

This Policy should be reviewed if there are any amendments in the regulatory guidelines and the revised policy should be staged for Board’s Approval in the subsequent Board Meeting post the amendments are notified by the regulator