REDICO VANIJYA PRIVATE LIMITED

Know Your Customer (KYC) and Prevention of Money Laundering (PML) Policy

Introduction

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

Objective

The KYC /AML policy is framed in line with RBI Direction / Prevention of the Money Laundering Act, 2002 /Rules as amended from time to time. The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. The KYC policy has been framed by the Company for the following purposes:

- To prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities;
- To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
- To enable Company to know and understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
- To put in place appropriate controls for detection and reporting of suspicious activities as envisaged under the Anti Money Laundering Act, 2002 and in accordance with laid down procedures;

- To comply with applicable laws and regulatory guidelines;

'Know Your Customer' Standards

The objective of KYC guidelines is to prevent NBFCs from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. Banks should frame their KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy;
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions;
(iv) Risk management;
(v) Training Programme;
(vi) Internal Control Systems;
(vii) Record Keeping;
(viii) Appointment of Principal Officer;
(ix) Reporting to Financial Intelligence Unit.

For the purpose of KYC policy, a 'Customer' may be defined as:

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e., the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

Customer Acceptance Policy (CAP)

The Company shall develop a clear Customer Acceptance Policy (CAP) laying down explicit criteria for acceptance of customers. The CAP must ensure that explicit guidelines are in place on the following aspects of customer relationship in the company:

- No account may be opened in an anonymous or fictitious/ benami name(s).
- The Company shall classify customers into various risk categories and based on risk perception decide on the acceptance criteria for each customer category.
- Accept customers only after verifying their identity as laid down in the customer identification procedures.
- While carrying out due diligence the Company will ensure that the procedures adopted will not result in the denial of services to genuine customers.
- For the purpose of risk categorisation of customers, the Company shall obtain the relevant information from the customer at the time of account opening.

Customer Identification Procedures (CIP)

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. It shall obtain sufficient information necessary to verify the identity of each new customer along with brief details of its promoters and management, whether regular or occasional and the purpose of the intended nature of the business relationship. The requirement as mentioned herein may be moderated according to the risk perception; for example, in the case of a public listed company it will not be necessary to identify all the shareholders. An indicative list of the nature and type of 8 documents/information that may be relied upon for customer identification is given in the Annex-II.

An indicative list of the nature and type of documents/information that may be relied upon for Customer identification is given in Annex-I. The Company will frame the internal guidelines based on its experience of dealing with such persons/entities, normal prudence and the legal requirements.

Persons who avail the loan facility from the company, the details of CIP and documents required are listed in Annex-I.

The Company shall periodically update Customer Identification Data after the transaction is entered. A system of periodic review of risk categorization of transaction or business relationship with such periodicity being at least once in six months and need for applying enhanced due diligence measures shall be put in place.

Monitoring of Transactions

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent logical or visible lawful purpose.

- Background of the customer,
- country of origin,
- sources of funds,
- the type of transactions involved and other risk factors shall determine the extent of monitoring.

Higher risk accounts shall be subjected to intensify monitoring. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

After due diligence at the appropriate levels in the company, transactions of suspicious nature and/or any other type of transaction notified under PML Act, 2002 will be reported to the appropriate authority and a record of such transaction will be preserved and maintained for a period as prescribed in the Act. It shall carry out the periodic review of risk categorization of transactions/customers and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

Risk Management

The Company shall adopt a risk-based approach to ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. Company will adhere to the following for effective implementation of Risk Management:

- Originals of the KYC documents shall be verified by officials of the Company and copies thereof shall be obtained and retained with the Company. Such copies shall be attested by the Company officials certifying that they have been verified with the originals.
- KYC documents so obtained shall be properly arranged and filed in order so that they shall be available for verification any time.

- Company's Internal Auditors shall ensure an independent evaluation of compliance of KYC/AML policy including legal and regulatory requirements. They shall report Lapses observed in this regard as Irregularities in their Audit Reports.
- Adverse features noted by the Internal Auditors shall be brought to the attention of the Principal Officer.
- Summary of serious Irregularities/deviations shall be placed before the Audit Committee of the Board by the Internal Audit Department at quarterly intervals.
- Review of implementation of KYC/AML guidelines shall also be placed before the Audit Committee of the Board by the Principal Officer at quarterly intervals.
- The Company shall have an on-going employee training programme so that members of the staff are adequately trained in KYC/AML procedures.
- The Principal Officer designated by the Company in this regard shall have responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML Policy.
- Designated Director shall be responsible for the overall compliance with the obligations under the Act and Rules.

Training Programme

Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/ staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC Policies and implement them consistently.

Internal Control System

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC Policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management of the Company under the supervision of the Committee shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the

application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Committee along with their normal reporting frequency. Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

Record Keeping

The Company shall maintain proper record of the transactions as required under Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules).

Records to contain the specified information The Records referred to above in Rule 3 of PML Rules to contain the following information:

- ❖ the nature of the transactions;
- ❖ the amount of the transaction and the currency in which it was denominated;
- ❖ the date on which the transaction was conducted;
- ❖ the parties to the transaction.

Maintenance and preservation of records Section 12 of PML Act requires the Company to maintain records as under:

- Maintain all necessary records of transactions between the Company and the Customer, both domestic and international, for at least five years from the date of transaction;
- Preserve the records pertaining to the identification of the customers and their addresses obtained during the course of Business relationship, for at least five years after the business relationship is ended;
- Make available the identification records and transaction data to the competent authorities upon request;
- Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

Appointment of Compliance Officer

The Company shall designate a senior employee as 'Compliance Officer' (CO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.

Reporting to Financial Intelligence Unit

The Compliance Officer shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI.

The employees of Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

Suspicious Transaction Report (STR)

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. "Reasonable grounds to suspect" is determined by what is reasonable in the circumstances, including normal business practices and systems within the industry.

There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour.

Money Laundering and Terrorist Financing Risk Assessment by REs

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

(b) The risk assessment by the company 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 should be reviewed at least annually.

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

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.

Prevention of Money Laundering Act, 2002 – Obligations of Company in terms of rules notified thereunder

Company has appointed "Principal Officer" who will put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. Further with the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

(a) issue a warning in writing; or

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

For the purpose of this policy, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of funds.

Money Laundering - Risk Perception

Following are the risks, which arise out of Money Laundering activities:

a. Reputation Risk - Risk of loss due to severe impact on reputation. This may be of particular concern given the nature of business, which requires the confidence of customers, and the general market place.

b. Compliance Risk - Risk of loss due to failure of compliance with key regulations governing the operations.

c. Operational Risk - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

d. Legal Risk - Risk of loss due to any legal action on company or its staff may face due to failure to comply with the law. Company should ensure to cover all the above stated risks and should have proper checks to control to combat the above stated risks.

Monitoring and Reporting of Cash Transactions

No cash of Rs. 50,000/- and above shall be accepted from a Customer/ any other intermediary (auction cases) without obtaining a copy of the PAN card of the Customer/any other intermediary. In case a customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

Any cash transactions of Rs. 10 lakhs and above and integrally connected cash transactions of Rs, 10 lakh and above per month shall be reported to FIU-IND by 15th of the succeeding month as CTR. For further details, Rules 3 to 8 (Appendix B) may be seen. The Company shall lay down proper mechanism to check any kind of attempts to avoid disclosure of PAN details. In case of possible attempts to circumvent the requirements, the same shall be reviewed from the angle of suspicious activities and shall be reported to FIU-IND, if required.

Annex-I

Customer Identification Procedure Features to be verified and Documents that may be obtained from customers:

- **KYC Documents for Individual:**

Sr. No.	KYC Documents (Officially Valid Documents)	ID Proof	Address Proof
1.	PAN Card	Acceptable (Mandatory)	Not Acceptable
2.	Driving License	Acceptable	Acceptable
3.	Valid Passport	Acceptable	Acceptable
4.	Aadhaar Card	Acceptable	Acceptable
5.	Voter's Identity Card issued by Election Commission	Acceptable	Acceptable
6.	Job Card issued by NREGA duly signed by an officer of the State Govt	Acceptable	Acceptable

- **KYC Documents for Proprietorship:**

Any two of the following documents in the name of the proprietary concern needs to be obtained if the loan is in the name of Proprietorship Firm (Main Applicant)

- Registration certificate (in the case of a registered concern);

- Certificate/licence issued by the municipal authorities under Shop and Establishment Act;
- Sales and income tax returns
- Certificate/registration document issued by Sales Tax/GST/Professional Tax authorities;
- IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;
- Latest Utility bills such as electricity, water, and landline telephone bills (should not be more than two months old). Latest Property Tax Receipt and Sale deed also.
- GST Registration Certificate.

➢ **KYC Documents for Companies:**

One certified copy of each of the following documents shall be obtained:

- Certificate of incorporation;
- Memorandum and Articles of Association;
- PAN card (Mandatory)
- A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
- GST Registration Certificate;
- An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf;

➢ **KYC Documents for Partnership Firms:**

One certified copy of each of the following documents shall be obtained:

- Registration Certificate;
- PAN card (Mandatory)
- Partnership Deed;
- GST Registration Certificate;
- An officially valid document in respect of the person holding an attorney to transact on its behalf;

Annex-II

Customer Identification Procedure

The customer identification procedure shall be as follows: Customer shall provide following documents (self-attested) in jpg format:

- Photo Identity Proof - PAN Card
- Permanent Address Proof - Anyone (1) of: Aadhar Card; Passport; Driving License; Voter's Identity Card.

Further where an Individual, who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and who does not submit Aadhaar or proof of application of enrollment for Aadhaar, the following shall be obtained:

- certified copy of an OVD containing details of identity and address and
- one recent photograph

If Current Address is different from Permanent Address, then additionally:

- Utility Bill- Electric/landline phone bill/ Gas Bill of current address (not more than 2 months old).
- Leave and License Agreement/Rent Agreement.
- Current Photograph as a selfie.
- Bank Account Statement

Further, UBFC also endeavours to adopt digital Customer Identification Process in line with prescribed guidelines issued by the Reserve Bank of India in this regard.