

CD EQUIFINANCE PRIVATE LIMITED

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

Details	Date
Reviewed, Adopted and Implemented on	January 16, 2026
Approved by Board Meeting Dated	January 16, 2026
Next Review on	FY 2026-2027

Contents

I. Preamble.....	3
II. Objective.....	3
III. 'Know Your Customer' Standards	3
IV. Customer Acceptance Policy (CAP)	4
V. Customer Identification Procedures (CIP)	5
VI. Monitoring of Transactions.....	9
VII. CENTRAL KYC RECORDS REGISTRY	10
VIII. EXISTING ACCOUNTS.....	10
IX. CONFIDENTIALITY OF INFORMATION	11
X. Risk Management	11
XI. Training Programme.....	11
XII. Internal Control System	11
XIII. Maintaince of Records of transactions	12
XIV. Designated Director and Principal Officer	12
XV. Reporting to Financial Intelligence Unit	13
XVI. Suspicious Transaction Report (STR).....	13
XVII. Money Laundering and Terrorist Financing Risk Assessment by REs.....	13
XVIII. Prevention of Money Laundering Act, 2002 – Obligations of Company in terms of rules notified thereunder ..	14
XIX. Money Laundering - Risk Perception	14
XX. Monitoring and Reporting of Cash Transactions.....	15

I. Preamble

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.

II. 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:

- a. To prevent criminal elements from using Company for Money Laundering and Terrorist Funding activities;
- b. To put in place an effective system and procedure for Customer identification and verifying its / his / her identity and residential address.
- c. 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;
- d. 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;
- e. To comply with applicable laws and regulatory guidelines;

III. '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 NBFC to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. NBFC has framed their KYC policies incorporating the following elements:

- a. Customer Acceptance Policy;
- b. Customer Identification Procedures;
- c. Monitoring of Transactions;
- d. Central KYC Records Registry
- e. Risk management;
- f. Training Programme;
- g. Internal Control Systems;

- h. Record Keeping;
- i. Appointment of Principal Officer;
- j. 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 NBFC;
- 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 NBFC, say, a wire transfer or issue of a high value demand draft as a single transaction.

IV. Customer Acceptance Policy (CAP)

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

- a. The Company shall not open any account in anonymous / fictitious / benami name(s), or in the name of criminal background or banned entities such as individual terrorists or terrorist organisations etc.
- b. The Company shall put in place a suitable system to ensure that the identity of the customer does not match with any individual or entity appearing in the sanctions lists as prescribed under applicable regulatory directions.
- c. Prior to carrying out business activity with any customer, the nature of business activity, location, mode of payment, volume of turnover, social and financial status etc., of such customer will be ascertained by the Company.
- d. The Company shall verify the identity and credentials of the customer using reliable and independent sources, as applicable:
 - i. Where a Permanent Account Number (PAN) is obtained, the same shall be verified through the verification facility of the issuing authority.
 - ii. Where an equivalent electronic document (e-document) is obtained, the digital signature shall be verified in accordance with the provisions of the Information Technology Act, 2000.
 - iii. Where Goods and Services Tax (GST) details are furnished, the GST number shall be verified through the search/verification facility of the issuing authority.
 - iv. The Company shall clearly define and document the circumstances under which a customer is permitted to act on behalf of another person or entity and shall conduct appropriate due diligence in such cases.
- e. The Company shall seek any optional / additional information after the account is opened only with explicit consent of the customer, in case requirement of such information is not specified in this Policy. Further in respect of joint accounts, customer due diligence will be done in respect of all the joint holders.
- f. The Company will classify customers into low, medium, and high-risk categories for monitoring purposes. Categorisation of customers will be done on a case-to-case basis and subject to the RBI Guidelines issued in this behalf. The nature and extent of due diligence will depend on the risk perceived by the Company. The Company may also prepare a profile for each new customer based on risk categorisation and such profile will be confidential.
- g. The Risk Management Committee, while reviewing the customers, will also carry out money laundering and terrorist financing risk assessment, at least once in a financial year, to identify, assess and take effective measures to mitigate such risks, if any.

- h. Where the Company forms a suspicion of money laundering or terrorist financing and reasonably believes that carrying out the CDD process may tip off the customer, the Company shall not pursue the CDD process and shall file an STR with FIU-IND.
- i. For the purpose of risk categorisation, individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk.
- j. The Company shall not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence 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 furnished to the Company.
- k. The Company shall allot a Unique Customer Identification Code (UCIC) while opening new customer accounts and shall apply customer due diligence measures at the said stage. In other words, if an existing KYC compliant customer desires to open another account with the Company, no fresh due diligence shall be conducted.

V. Customer Identification Procedures (CIP)

Due care will be exercised to establish the identity of each new customer such that the Company is in a position to satisfy the competent authorities that due diligence was exercised in establishing the identity of the customers before opening any customer account.

For establishing the identity of the customer, it is necessary that the customer's name, address etc. are verified through proper documents.

The Company shall not seek or rely upon introduction from any person for the purpose of opening an account or establishing a customer relationship. But may rely on customer due diligence carried out by a third party, subject to compliance with applicable regulatory requirements. The Company shall obtain the CDD records immediately from such third party or from the Central KYC Records Registry (CKYCR). The Company shall ensure that the third party is regulated, supervised or monitored for compliance with KYC and record-keeping requirements under the PML Act, is not based in a high-risk jurisdiction, and makes available copies of identification data upon request without delay. The ultimate responsibility for customer due diligence and enhanced due diligence shall remain with the Company.

The Company shall apply enhanced due diligence in respect of foreign Politically Exposed Persons (PEPs) and adopt a risk-based approach for domestic Politically Exposed Persons (PEPs), in accordance with applicable regulatory requirements.

It is also necessary to determine whether a client is acting on behalf of a beneficial owner in terms of the PMLA, and identify the **Beneficial owner**, and take steps to verify the identity of the beneficial owner. Identification of beneficial owner, as stated above, will not be required in case the client is a

- listed company, or
- An entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
- subsidiary of such listed company.

Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

- Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
- "Control" shall include the right to appoint majority of the directors or to control the management or

policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

- b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

- c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent 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 percent 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.

In case of legal entities, besides the verification of name, address etc., it is also necessary to verify the status of the legal entity and its ownership & control structure, to determine who are the natural persons ultimately controlling the legal entity, and whether any person purporting to act on behalf of the legal person / entity is so authorised.

Such customer identification procedure will become imperative while carrying out the following transactions-

- Commencement of an account-based relationship with the customer.
- Transaction of an amount equal to or exceeding Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, for a non-account-based customer.
- International money transfer operations for a person who is not an account holder.
- When there is doubt about the authenticity or adequacy of the customer identification data that has been obtained.
- Transactions involving sale of third-party products as agents, sale of own products etc. having value of more than Rs. 50,000/-.
- When the Company has reasons to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

Customer identification in respect of entities requiring an extra element of caution, as per RBI requirements, are to be carried out in accordance with the RBI Guidelines issued in this behalf. It shall also be ensured that the identity of the customer does not match with any person or entity whose name appears in the **sanctions list** as specified in the RBI KYC Directions.

Copies of documents mentioned below for different categories of customers are to be obtained prior to opening a customer account for carrying out transactions with such customers.

All copies must be verified from the originals. For the purpose of this Policy, the term '**officially valid document**' shall include Passport/PAN Card / Voters Identity Card issued by the Election Commission of India / Driving licence / Job card issued by NREGA duly signed by an officer of the State Government / proof of possession of Aadhaar Number or any other document as may be notified under the RBI KYC Directions, PMLA & the Rules thereunder. A document shall be deemed to be an officially valid document even if there is any change in name, provided the same is supported by a marriage certificate issued by the State Government or Gazette Notification indicating such name change.

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.

Provided 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:-

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- Property or Municipal tax receipt;
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- 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 licence agreements with such employers allotting official accommodation;

The customer shall submit OVD with current address within a period of three months of submitting the documents above.

Also, where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: 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.

Below documents are mandatory be obtained while opening of account of customer with the company:

a. Individuals

- Certified copy of an officially valid document containing details of identity and address.
- Recent passport size photograph of the individual.
- PAN Card of the individual.
- Income tax return or any other proof of income.

b. Companies

- Certificate of incorporation and Memorandum & Articles of Association.
- Certified copy of the Board resolution for opening a customer account, if applicable.
- Power of Attorney, if any, granted to directors, managers, officers, or employees to transact business on behalf of the company or certified copy of the Board resolution for this purpose.
- PAN Card of the company.
- List of the directors along with their residential addresses.
- List of persons holding senior management in the company.
- Latest Shareholding pattern.
- Address of registered office and principal place of business (if it is different from registered office).
- Certified copy of an officially valid document containing details of identity, and address, one recent photograph, and PAN Numbers of directors, managers, officers, or employees authorised to transact business on behalf of the company.

The name and address, the principal place of business, telephone / fax number, control structure etc. are to be verified from the above-mentioned documents.

c. Sole proprietorship firm

- Certified copy of an officially valid document containing details of identity and address, one recent photograph and PAN Number of the proprietor.
- Any two of the following documents as proof of business / activity –
 - i. Registration certificate including Udyam Registration Certificate issued by Government.
 - ii. Certificate / licence / registration document issued by the municipal authorities under Shop and Establishment Act or issued by goods and services tax (GST) / professional tax authorities.
 - iii. Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
 - iv. GST returns
 - v. Complete income tax return of the proprietor where the firm's income is reflected along with proof of submission with the Income tax authorities.
 - vi. Utility bills such as electricity, water, and landline telephone bills and
 - vii. Importer Exporter Code issued to the proprietary concern by the Director General of Foreign Trade.

d. Partnership firm

- Registration Certificate, if the partnership firm is registered.
- Partnership Deed.
- PAN Card of the partnership firm.
- Power of Attorney granted to partners or officers / employees of the firm to transact business on behalf of the firm.
- GST Registration Certificate
- List of the Partners / persons holding the Power of Attorney, along with their residential addresses and certified copies of officially valid documents containing details of identity and address, one recent photograph, and PAN Numbers.
- Address of registered office and principal place of business (if it is different from registered office).
- Utility Bill which is not more than 2 months old of any service provider (electricity, telephone, postpaid mobile phone, pipe gas etc.) / Registered rental or lease or purchase agreement / Property or Municipal tax receipt / documents issued by Government departments of foreign jurisdiction and letters issued by Foreign Embassy or Mission in India in the name of firm / partners.

e. Trusts & Foundations

- Registration Certificate, if the Trust / Foundation is registered.
- Trust Deed.
- PAN Card of the trust.
- Resolution of the governing body of the Trust for opening a customer account with the Company.
- Power of Attorney granted to trustees / officers to transact business on behalf of the Trust / Foundation.
- Names of beneficiaries, trustees, settlor, protector, if any and authors of the trust.
- Address of the registered office of the trust.

List of the trustees/ officers holding the Power of Attorney, along with their residential addresses and copies of their officially valid documents containing details of identity and address, one recent photograph, and PAN Numbers. Further, the trustees shall disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as defined in clauses (ii), (iii) and (vi) under the Customer Identification Process.

f. Unincorporated associations or body of individuals

- Resolution of the managing body of the association or body of individuals for opening a customer account with the Company.
- PAN Card of the unincorporated association or body of individuals.

- Power of Attorney granted to officers / employees of the association / body of individuals to transact business on behalf of the association or body of individuals.
- List of the persons holding the Power of Attorney, along with their residential addresses and copies of their officially valid documents containing details of identity and address, one recent photograph, and PAN Numbers.

g. Other juridical persons entities not covered above

In case of a juridical person / entity not covered above such as societies, universities and local bodies like village panchayats etc. or who purports to act on behalf of such juridical person or individual or trust, the following documents will be required:

- Document showing name of the person authorised to act on behalf of the entity.
- Officially valid documents for proof of identity and address in respect of the person holding a power of attorney to transact on behalf of the entity.

The categories of customers mentioned above, and documents listed therein are only an indicative list of the nature of customer and type of documents / information that are to be relied upon for customer identification.

In case the document furnished by the customer does not contain the updated address, any of the following documents shall be taken for the limited purpose of proof of address — (a) Utility Bill which is not more than 2 months old of any service provider (electricity, telephones post-paid mobile phone, pipe gas, water bill etc.), (b) property or municipal tax receipt, (c) pension or family pension payment orders issued to retired

employees by Govt. Departments, and (d) letters of allotment of accommodation from employer. The customer shall submit updated officially valid document with current address within three months from submitting the aforesaid document. Further, in case of change in address, the customers shall submit fresh proof of address within six months.

In case of customers which are non-profit organisations, the Company will ensure that the details of such customers are registered on the DARPAN Portal of NIT' Aayog. Such registration records shall be preserved for a period of five years after the business relationship with such customer has ended or the account has been closed, whichever is later.

h. Politically Exposed Persons (PEPS)

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

Apart from performing normal customer due diligence, the Company will ensure to identify relationship of a Customer with PEP, if any, in terms of RBI KYC Directions

VI. Monitoring of Transactions

Customer transactions will be monitored in the following manner:

- a. All transactions will be monitored on an ongoing basis so that transactions that fall outside the regular pattern of activity can be identified. All transactions will also be examined to ensure that they are consistent with the Company's knowledge of the client, his / her business and risk profile, and where necessary, the source of funds.
- b. No Cash transactions will be entered into with any customer.
- c. The following types of transactions shall be closely monitored

- 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.
 - Transactions which exceed the thresholds prescribed for specific categories of accounts.
- d. While entering into transactions, key indicators of the customer such as the country of origin, sources of funds, the type of transaction involved, and other risk factors may be looked into.
 - e. Review of risk categorisation of accounts will be carried out by the Risk Management Committee of the Company on a yearly basis and based on such review, enhanced due diligence measures may be put in place. 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. Record of customer information transactions prescribed under the PMLA will be preserved, in hard or soft format, and maintained for a period of five years from the date of cessation of transaction.
 - g. When there is suspicion of money laundering or financing of activities relating to terrorism or where there is doubt about the adequacy or veracity of previously obtained client identification data, the Company shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.
 - h. In case there are reasons to suspect that any transactions with customers are of suspicious nature, including suspicion of money laundering or terrorist financing, then such transactions and all other transactions notified under the PMLA are to be reported to the appropriate authority. However, there should not be any restriction on operations in the accounts merely based on such reporting.
 - i. The Company will ensure that it does not open account in the name of any individual / entity whose name appears in the list of individuals and entities suspected of having terrorist links, as circulated by the RBI or any other regulatory authority. For this purpose, the Company will run a check on the prescribed parameters at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the Company. In case of any match, the Company will immediately report the same to the appropriate authority.

VII. CENTRAL KYC RECORDS REGISTRY

The Company shall comply with all applicable rules and regulations relating to submission of KYC data to and retrieving KYC data from the records of the Central KYC Records Registry. Company shall capture customer KYC records and upload into CKYC Records within 10 days of commencement of an account-based relationship with the customer.

VIII. EXISTING ACCOUNTS

This Policy is applicable to all existing Accounts (if any) based on risk profile of the customer. The Company shall adopt risk-based approach for periodic updation of KYC. In case of existing Accounts, periodic updation of KYC will be done as follows:

- at least once in every 2 years for high-risk individuals and entities.
- at least once in every 8 years for medium risk individuals and entities; and
- at least once in every 10 years for low-risk individuals and entities.

Fresh proofs of identity and address will not be required if there is no change in KYC information of the customers as available with the Company. A self-declaration by the customer to this effect will suffice and physical presence of such customer shall not be insisted upon. In case of change in only address details, a self-declaration of the new address will be obtained, and the declared address will be verified. PAN details of the customer will also be verified from the database of the issuing authority at the time of periodic updation of the KYC. Further, in case the validity of the documents available with the Company has expired at the time of periodic updation of the KYC, the Company shall undertake fresh KYC process equivalent to that applicable to a new customer.

- In case of non-individual customers, the Company shall also verify the status of their beneficial owner(s) and update the same, if required. Fresh photographs will be obtained from minor customers on attaining majority and fresh KYC for such customers will be carried out.

The Company will provide acknowledgement to the customer for carrying out such periodic updation, mentioning the date of receipt of the relevant document(s) including self-declaration from the customer. The information / documents obtained from the customers will be promptly updated in the records and an intimation mentioning the date of updation of KYC details will be provided to the customer.

The Company will also advise its customers that in case of any update in the documents submitted by them at the time of establishment of business relationship / account-based relationship and thereafter, they shall submit the updated documents to the Company within 30 days of such update.

IX. CONFIDENTIALITY OF INFORMATION

- a. Information collected by the Company from its customers in terms of this Policy shall be treated as confidential and details thereof shall not be divulged for any purpose, without the explicit consent of the customer. However, the said restriction will not be applicable to cases where disclosure is required under compulsion of law or there is a duty to the public to disclose or where disclosure is required to be made in the interest of the Company or where such disclosure is made with the express or implied consent of the customer.
- b. The Company shall ensure that the fact of maintenance of records and furnishing of information to the concerned authorities in terms of the PMLA will remain confidential. However, such confidentiality requirement shall not prohibit sharing of information under the RBI KYC Directions for any analysis of transactions and activities which appear unusual, if any such analysis has been done.

X. Risk Management

Adherence to KYC Policy will be checked during the Internal Audit of the Company and the Internal Audit Report will be put up to the Audit Committee. Compliance of the PMLA and the Rules thereunder will form part of the Quarterly Statutory Compliance Report of the Company placed before the Board.

XI. Training Programme

Company has 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.

XII. Internal Control System

The Company's Internal control 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 ensure that the audit function is staffed adequately with skilled individuals. Internal Control will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. Further, the Company 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.

XIII. Maintenance of Records of transactions

The Company is maintaining 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:

- a. Nature of the transactions;
- b. Amount of the transaction and the currency in which it was denominated;
- c. Date on which the transaction was conducted;
- d. Parties to the transaction.
- e. Maintenance and preservation of records Section 12 of PML Act requires the Company to maintain records as under:
- f. 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;
- g. 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;
- h. Make available the identification records and transaction data to the competent authorities upon request;
- i. Company takes 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.

XIV. Designated Director and Principal Officer

a. Designated Director:

- A "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.
- 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'.

b. Principal Officer:

- The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- 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 Principal Officer shall also be communicated to the RBI.

XV. Reporting to Financial Intelligence Unit

The Compliance Officer Reports 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.

To facilitate effective identification and reporting of suspicious transactions, the NBFC shall implement robust software systems that generate alerts for transactions inconsistent with a customer's risk categorisation and updated profile.

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

XVI. 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.

XVII. Money Laundering and Terrorist Financing Risk Assessment by REs

- a. The Company 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 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 is applying 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.

XVIII. 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.”
- e. 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.

XIX. 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.

XX. Monitoring and Reporting of Cash Transactions

No cash is 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.