



Veritas Finance Private
Limited – KYC Policy

Version 7.0 : 25.04.2024

VERITAS FINANCE PRIVATE LIMITED

KYC POLICY

Version Control	Document name	Date of approval
1.0	Veritas Finance Private Limited KYC Policy	28.03.2016
2.0	Veritas Finance Private Limited KYC Policy	12.10.2018
3.0	Veritas Finance Private Limited KYC Policy	08.10.2020
4.0	Veritas Finance Private Limited KYC Policy	20.01.2021
5.0	Veritas Finance Private Limited KYC Policy	07.06.2023
6.0	Veritas Finance Private Limited KYC Policy	30.01.2024
7.0	Veritas Finance Private Limited KYC Policy	25.04.2024

KYC POLICY

S.No.	Particulars	Page No.
1	Introduction	4
2	Regulatory Framework	4
3	Definitions	4
4	Money Laundering and Terrorist Financing Risk Assessment	7
5	Key Elements for KYC Procedures	8
6	Enhanced Due Diligence	14
7	Appointment of Designated Director / Principal Officer	14
8	Maintenance of Records	14
9	Secrecy Obligations and Sharing of Information	16
10	FATCA and CRS reporting	16
11	Reporting to Financial Intelligence Unit – India	16
12	Combating Financing of Terrorism	16
13	Customer Education/Employee's training/Employee's hiring	17
14	General	17



Details of Amendments in Version 7.0		
Sl.No	Items	Pg. No
1	Inclusion of FATCA and CRS reporting	16

1) Introduction

Veritas Finance Private Limited (VFPL) is focused on meeting the financial needs of the micro, small and medium enterprises (MSME) in India, which has remained largely underserved despite several initiatives. This policy is applicable to all categories of products and services offered by the Company.

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Master Directions 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 (Refer RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16, updates as of Jan.2024)

The KYC and AML policy shall broadly cover

- a) Process to determine the identity of customer, nature of business, reasonableness of operations which in turn helps us to manage our risks prudently.
- b) Shall place appropriate controls for detection and reporting of suspicious activities.
- c) Ensure that all the VFPL staffs are adequately trained in KYC and AML procedures.

2) Regulatory framework

In line with the above, VFPL shall follow customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. VFPL shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of any such amendment(s).

In compliance with the guidelines, the following KYC & AML policy of Veritas Finance Private Limited (herein after referred to as 'Company') is approved by the Board of Directors.

3) Definitions

3.1) Beneficial Owner (BO)

A list of persons who are to be considered as BOs in relation to a customer is given below:

Type of Customer	Persons to be considered Beneficial Owners (BOs)
Public / Private Limited Companies	<ol style="list-style-type: none"> a) If the customer is a company, whether alone or together, or through one or more juridical person, ownership of or entitlement to more than 10% of shares or capital or profits of the Company; or b) "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.

Partnership Firm	a) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership.
Unincorporated association of persons or body of individuals	a) 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 per cent of the property or capital or profits of the unincorporated association or body of individuals.
Trust/ Foundation	a) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3.2) Customer - Means a person who is engaged in a financial transaction or activity with Veritas Finance and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.3) Customer Due Diligence (CDD) - Identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents (OVD)' as a 'proof of identity' and a 'proof of address'.

3.4) Customer identification - means undertaking the process of CDD.

3.5) Officially valid document (OVD)

a) Following documents as mentioned in OVD shall be obtained from all borrowers and co-borrowers.

SI.No	KYC Document
1	Passport
2	Voter ID Card (only if it contains the current address)
3	Driving License
4	Job card issued by NREGA duly signed by State govt officer
5	PAN Card or Form 60*
6	Letter issued by National Population Register
7	Proof of possession of Aadhaar (As per UIDAI, AADHAR card can be used as OVD only on masking the number)

**OVD need to be collected for all the borrowers.*

**In the absence of Permanent Account Number (PAN) , Form 60 shall be collected for borrowers and co-borrowers.*

*** Affidavit with Self-declaration shall be obtained in case the current address differs from the address in Aadhaar Card*

- b) If the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:
- I. Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - II. Property or Municipal Tax receipt;
 - III. Bank account or Post Office savings bank account statement;
 - IV. Pension or family Pension payment orders (PPOs) issued to retired employees by Government Departments or PSUs, if they contain address.
 - V. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and vi. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.
- c) The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- d) Where the OVD presented by a foreign national(NRI) 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 shall be accepted as proof of address

3.6) Person” - means and includes:

- a) an Individual
- b) A Hindu Undivided Family,
- c) A Company
- d) A Firm
- e) an association of persons or a body of individuals, whether incorporated or not,
- f) every artificial juridical person, not falling within any one of the above persons (a to e), and
- G) any agency, office or branch owned or controlled by any of the above persons (a to f)

3.7) Central KYC Records Registry (CKYCR)

KYC data collected are collated and reported to CKYCR for all borrowers. The captured customer's KYC records has to be uploaded onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

3.8) Designated Director means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

3.9) Politically Exposed Persons (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.

3.10) Principal Officer means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

3.11) Reporting Entity for the purpose of this Policy would mean the Company, Veritas Finance Private Limited(VFPL)

3.12) Suspicious transaction means a “transaction”, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to not have economic rationale or bona-fide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

3.13) Equivalent e-document means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities)Rules, 2016.

4) MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT:

As per the RBI notification on the KYC amendment dated January,2024, the KYC policy of the company includes the amendment with regard to Money Laundering and Terrorist Financing Risk Assessment by the Regulated Entities (VFPLs).

a. VFPLs 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, company 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 or any committee of 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.

Company shall apply a Risk Based Approach (RBA) and implement a CDD programme regard to ML/TF for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, company shall monitor the implementation of the controls and enhance them if necessary.

5) KEY ELEMENTS for KYC Procedures:

KYC procedures also enable us to know/understand our customers and their financial dealings better which in turn help them manage their risks prudently. We have framed our KYC policy incorporating the following four key elements:

- Customer Acceptance Policy
- Risk Management
- Customer Identification Procedure
- Monitoring of Transaction and

5.1) CUSTOMER ACCEPTANCE POLICY

The Company shall follow the following norms while accepting and dealing with its customers:

1. No account is opened in anonymous or fictitious/benami name.
2. No account is opened where the Company is unable to apply appropriate CDD (Customer Due Diligence) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
3. No transaction or account based relationship is undertaken without following the CDD procedure.
4. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
5. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
6. The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a Company desires to open another account with the same Company, there shall be no need for a fresh CDD exercise.
7. CDD Procedure is followed for all the joint account holders, while opening a joint account.
8. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
9. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
10. Where Goods and Services Tax (GST) details are obtained, the same shall be verified from the search/verification facility of the issuing authority.
11. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
12. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.

5.2) RISK MANAGEMENT

- The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.
- Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures.
- As a general rule, the compliance function also provides an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements.
- The compliance in this regard is put up before the Audit Committee of the Board on quarterly intervals.

5.2.1) Risk Categorization:

The Company has a system in place for periodical updation of customer identification data after the account is opened.

5.2.2) Indicative List of Risk Categorization:**a) Low Risk Category**

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 is categorized as low risk. (In all probabilities the Company is doing and will continue to do their business with such category of customers)

Examples of customers requiring Lower due diligence may include

1. Salaried employees with well-defined salary structures;
2. People working with government owned companies, regulators and statutory bodies, etc.;
3. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
4. People working with Public Sector Units;
5. People working with reputed Public Limited Companies and Multinational Companies

b) Medium Risk Category

Customers who are likely to pose a higher than average risk may be categorized as medium risk category

Examples of customers requiring medium due diligence may include

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

c) High Risk Category

Categorization of high risk shall be depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Examples of customers requiring higher due diligence may include:

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

5.3) Customer Identification Procedure

Identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

The Company shall undertake identification of customers in the following cases:

- (a) Commencement of an account-based relationship with the customer.
- (b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

The customer identification will be through an introductory reference from an existing customer with a satisfactorily conducted loan account or a person known to us and on the basis of documents provided by the customer or through staff members knowing the potential customer or any other document for identification and proof of residence.

5.3.1 Identification:

The company shall obtain the following information from an individual while establishing an account based relationship with:

A. Individual

1. Permanent Account Number (PAN) (in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained)
2. Passport
3. Voter's Identity Card
4. Driving License
5. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company.

For the purpose, Veritas can also obtain KYC with explicit customer consent via OTP to download KYC records from CKYCR, for the purpose of CDD. KYC document downloaded from CKYCR cannot be used if the validity has lapsed. If the KYC is obtained from CKYCR, then information of CDD carried out by them can be obtained immediately.

The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

B. Proprietary Firms

1. Permanent Account Number (PAN) (in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained)
2. Registration Certificate
3. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
4. Sales and income tax returns.
5. CST/VAT/ GST certificate (provisional/final).
6. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

7. 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.
8. Utility bills such as electricity, water, and landline telephone bills
9. Telephone/Fax number/E-mail ID;
10. Recent color photograph
11. Registration certificate as a proof of business/activity in the name of the proprietary firm includes “Udyam Registration Certificate (URC) issued by the Government.

In cases where the Company is satisfied that it is not possible to furnish two such documents as proof of business along with PAN number of individual, the Company may, at their discretion, accept only one of those documents as proof of business/activity. Provided the Company undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

C. Company

1. Certificate of incorporation
2. Memorandum and Articles of Association.
3. Permanent Account Number of the company.
4. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
5. Identification information i.e. PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
6. Names of the relevant persons holding senior management position.
7. Registered office and the principal place of its business, if it is different.

D. Partnership Firms

1. Registration certificate
2. Partnership deed
3. Permanent Account Number of the partnership firm.
4. Identification information i.e. PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5. Names of all the partners
6. Address of the registered office, and the principal place of its business, if it is different.

E. Trust

1. Registration certificate
2. Trust deed.
3. Permanent Account Number or Form 60 of the trust.
4. Identification information i.e. PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.
5. Names of the beneficiaries, trustees, settlor and authors of the trust.
6. Address of the registered office of the trust, and
7. List of trustees and documents, as specified in Section 16, for those discharging role as trustee and authorised to transact on behalf of the trust.

F. Unincorporated association or body of individuals:

1. Resolution of the managing body of such association or body of individuals
2. Permanent Account Number or Form 60 of unincorporated association or body of individuals.
3. Power of attorney granted to him to transact on its behalf
4. An officially valid document in respect of the person holding an attorney to transact on its behalf.
5. Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals

Other than list of documents mentioned under OVD or KYC list are not considered as Originally Valid Documents as per KYC Master directions of RBI.

5.3.2 Verification

Verification of customer identity should occur before transacting with the customer. The Company describes the acceptable methods of verification of customer identity, which includes verification through documents or non-documentary verification methods that are appropriate and the associated risks.

5.4) Monitoring of transaction:**A) Ongoing due diligence:**

On-going monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts have to be subjected to intensified monitoring.

The Company shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. For ongoing due diligence, VFPL shall adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

The periodicity of such updation is not less than once in ten years in case of low risk category customers and not less than once in two years in case of high and once in eight years for medium risk categories.

Individual customers	
a) No change in KYC information	A self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, or OTP consent with customer's mobile number registered with the Company, digital channels (such as mobile application of Company), letter etc.
b) Change in address	<p>a) A self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company or customer's mobile number registered with the Company, digital channels (such as mobile application of Company), letter etc.</p> <p>b) The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of new address, declared by the customer at the time of periodic updation and the same shall be verified through positive confirmation within two months of customer declaration.</p>
c) Additional measures	<p>a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC processequivalent to that applicable for on-boarding a new customer.</p> <p>b) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.</p> <p>c) In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.</p> <p>d) Risk based approach for periodic updation of KYC, ensuring that the information or data collected under CDD is kept relevant and up-to-date, particularly for high risk customers.</p>

6) Enhanced due diligence:

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

6.1) Existing Customer:

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

6.2) Reliance on third party due diligence:

The company shall not rely on third party due diligence.

7) Appointment of designated director / principal officer

The Board of Directors shall nominate a “Designated Director” to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The “Designated Director” can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the “Designated Director”. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

Mr. D. Arulmany, Managing Director & CEO will be the Designated Director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Mr. J. Prakash Rayen is designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

As per the RBI guidelines, the Principal Officer is located at our corporate office and is responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He maintains a close liaison with enforcement agencies, other NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

8) Maintenance of Records of Transactions/Information to be preserved:

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

(i) Maintenance of records of transactions

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

- All cash transactions of the value of more than Rs. 10 lacs, though by policy the Company does not accept cash deposits in foreign currency.
- All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lacs where such series of transactions have taken place within a month.
- All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.

- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transaction:
 - All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.
 - An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure III
- a) Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- b) Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
 2. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
 3. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- c) Certain Employees of the Company arousing suspicion:
1. An employee whose lavish lifestyle cannot be supported by his or her salary.
 2. Negligence of employees/wilful blindness is reported repeatedly.
- d) Some examples of suspicious activities/transactions to be monitored by the operating staff:
1. Multiple accounts under the same name
 2. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc;
 3. There are reasonable doubts over the real beneficiary of the loan
 4. Frequent requests for change of address

(ii) Information to be preserved:

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

1. the nature of the transactions;
2. the amount of the transaction and the currency in which it was denominated;
3. the date on which the transaction was conducted;
4. the parties to the transaction.

(iii) Maintenance and preservation of records:

The company has a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. The company will maintain for at least five years from the date of cessation of transaction between the company and the customer, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The company also ensures that records pertaining to the identification of the customer and his/ her address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the loan account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.

9) Secrecy obligations and sharing of information

Customer information obtained for account opening shall be kept private and confidential; details won't be shared with third parties for the purpose of cross-selling or for any other reason without the customer's express consent. While considering the requests for data/information from Government and other agencies, REs must ensure that the information being sought does not breach any legal requirements pertaining to transaction secrecy.

The exceptions to the said rule shall be as under:

1. Where disclosure is under compulsion of law
2. Where there is a duty to the public to disclose
3. the interest of company requires disclosure and
4. Where the disclosure is made with the express or implied consent of the customer

10) FATCA and CRS reporting:

In line with regulatory guidelines, all account holder needs to provide a FATCA/ CRS declaration/ self-certification form apart from regular KYC information at the time of on-boarding. A loan account becomes reportable under FATCA/CRS if the account holder/controlling persons are tax residents of any country other than India.

11) Reporting to Financial Intelligence Unit – India

a) In accordance with the requirements under PMLA, the Principal Officer of Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND): a. Cash Transaction Report (CTR) - If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

b) Counterfeit Currency Report (CCR) - All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

c) Suspicious Transactions Reporting (STR) - The Company will endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to FIU-IND. The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally

12) Combating Financing of Terrorism

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

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by ReserveBank, the Company shall ensure to update the consolidated list of individuals and entities as circulatedby Reserve Bank. The Company shall, before opening any new account, ensure that the name/s of the proposed customer does not appear on the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing

resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the Company as an integral part of recruitment/hiring process of personnel.

13) Customer Education/Employee's training/ Employee's Hiring:**a) Customer Education:**

The frontline staffs are specially trained to handle such situations while dealing with customers. The Company takes care to see that implementation of the KYC guidelines in respect of customer acceptance, identification etc. do not result in denial of opening of new loan accounts to general public. Any changes amended on considering regulatory aspect, the same will be communicated to customer on considering the relevance and importance of KYC.

b) Employee's Training:

The Company must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

There should be open communication, high-integrity, proper understanding of subject matter amongst the Company's staff dealing with KYC/AML matters.

14) General:

a. Closure of Accounts/Termination of Financing/Business Relationship Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the Company shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of the key managerial persons authorized for the purpose.

b. KYC for the Existing Accounts: While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions with existing customers would be continuously monitored for any unusual pattern in the operation of the accounts.

c. Updation in KYC Policy of Company Principal Officer after taking the due approval from the Board of Directors of the Company shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time