VERITAS FINANCE LIMITED

KYC AND AML POLICY

Version Control	**Document name**	**Date of approval**
1.0	Veritas Finance Limited KYC Policy	28.03.2016
2.0	Veritas Finance Limited KYC Policy	12.10.2018
3.0	Veritas Finance Limited KYC Policy	08.10.2020
4.0	Veritas Finance Limited KYC Policy	20.01.2021
5.0	Veritas Finance Limited KYC Policy	07.06.2023
6.0	Veritas Finance Limited KYC Policy	30.01.2024
7.0	Veritas Finance Limited KYC Policy	25.04.2024
8.0	Veritas Finance Limited KYC AND AML Policy	29.10.2024
9.0	Veritas Finance Limited KYC & AML Policy	05.02.2025
9.0(Policy Renewal)	Veritas Finance Limited KYC & AML Policy	30.04.2025
10.0	Veritas Finance Limited KYC & AML Policy	13-08-2025
11.0	Veritas Finance Limited KYC & AML Policy	29-10-2026

Revision History

Version no	Date	Revision details
5	07.06.2023	Amendment based on Reference - Master Direction DBR.AML.BC.No.81/14.01.001/2015 16 Amendment dated April 28,2023 • Beneficial ownership interest % • List of KYC documents • Customer acceptance policy 1) Additional KYC consent 2) GST number acceptance • Risk categorization: Additional parameters • Customer due diligence 1) Additional documents for Non individuals & Individuals • Ongoing Due Diligence • Periodic updation of KYC • Enhanced Due Diligence: Non face to face customers onboarding
6	30.01.2024	• Modifications in beneficial owner threshold for partnership firm • Inclusion of CKYC Registry, Equivalent e-document as KYC, Under Definitions – Inclusion of Politically Exposed Persons (PEP) • List of KYC documents – updated OVD list as per RBI norms • Money Laundering & Terrorist Financing Risk Assessment – Inclusion of Risk Based Approach • Customer Acceptance Policy – included GST verification and equivalent e-document verification • Periodic Updation of KYC under ongoing due diligence – Inclusion of Risk Based approach for high risk customers • Maintenance of Records for all cash transactions of value above 10 lacs. • Inclusion of Secrecy Obligations & Sharing of Information • Inclusion of Customer Education/Employee's Training/ Employees Hiring
7	25.04.2024	• Inclusion of FATCA and CRS reporting
8	29.10.2024	• UCIC and Deduplication- defined and process explained • Updated Risk Categorization-revisited risk categorization in line with Re KYC simplified measures notification by RBI • Process of Risk Categorization- procedure on how risk is categorized is included • Customer Screening-modality of customer screening is included • Client account opened by professional intermediaries -included and clarified as per RBI directives • CKYCR-elaborated as per RBI directives • Process of monitoring and reporting suspicious transaction • EDD- Scope defined

9	05.02.2025	• Updated OVD list – Aligned with KYC AML Master Direction • Central KYC Records Registry (CKYCR) Compliance (Paragraph 56 of MD)- REs are required to upload KYC records for individual customers and legal entities to CKYCR. KYC updates must be provided within seven days or as notified. This ensures centralized KYC records are accessible for future verification and that customers aren't required to resubmit identical documents • KYC Identifier and Document Submission (Paragraph 56(j) of MD) - When an RE has a customer's KYC identifier, additional KYC documents are not required unless there is updated information, incomplete records, expired document validity or a need for enhanced due diligence
9	30.04.2025	• Policy Renewal • Clarification regarding the interpretation of PAN requirements has been incorporated
10	13.08.2025	• Incorporated guidelines for advance intimation and post-due reminders to customers regarding periodic KYC updation • Escalation mechanism for customer support in periodic KYC updation **To be implemented on or before 1st January 2026*
11	29.10.2026	• Amendments to incorporate provisions in U.S.A. w.r.t. Anti-money laundering regulations • Updating Form 97 reference against erstwhile Form 60 • Clarification on approach of grey and black list countries for NRI loans

KYC AND AML POLICY

S.No.	Particulars	Page No.
1	Introduction	5
2	Regulatory Framework	5
3	Definitions	6
4	Money Laundering and Terrorist Financing Risk Assessment	9
5	Key Elements for KYC Procedures	10
6	Enhanced Due Diligence	24
7	Appointment of Designated Director / Principal Officer	25
8	Maintenance of Records	25
9	Secrecy Obligations and Sharing of Information	27
10	FATCA and CRS reporting	28
11	Reporting to Financial Intelligence Unit – India	28
12	Combating Financing of Terrorism	28
13	Customer Education/Employee's training/Employee's hiring	29
15	International AML , CFT, Proliferation Financing and Financial Sanctions Compliance	30
16	General	34

1) Introduction

Veritas Finance Limited (VFL) 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 Reserve Bank of India has amended the existing MD on KYC vide Notification RBI/2024-2025/87 DOR.AML.REC.49/14.01.001/2024-25 dated 6th November 2024 to

(a) align the instructions with the recent amendments carried out in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 vide Gazette Notification dated July 19, 2024,

(b) incorporate instructions in terms of the corrigendum dated April 22, 2024 issued by the Government of India to the Order dated February 2, 2021 on the *'Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967'*, and

(c) revise certain existing instructions. The changes carried out in the Master Direction are provided in Annex. The amended provisions in the Master Direction has come into force with immediate effect.

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 VFL staff are adequately trained in KYC and AML procedures.

2) Regulatory framework

In line with the above, VFL shall follow customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise monitoring their transactions. VFL 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 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	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) The following documents as mentioned in OVD shall be obtained from all borrowers and co-borrowers.

SI.No	KYC Document	ID Proof	Sign proof	Address proof	Age proof
1	Passport	Yes	Yes	Yes	Yes
2	Voter ID Card	Yes	No	Yes	Yes
3	Driving License	Yes	Yes	Yes	Yes
4	Job card issued by NREGA duly signed by State govt officer	Yes	No	No	Yes
5	Letter issued by National Population Register	Yes	No	Yes	Yes
6	Proof of possession of Aadhaar (As per UIDAI, AADHAR card can be used as OVD only on masking the number)	Yes	No	Yes	Yes
Mandatory Document					
1	PAN Card or Form 97*	a) Permanent account number (PAN) shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks/NBFCs, as amended from time to time. b) Form 97 shall be obtained from persons who do not have PAN or equivalent e-document thereof.			

**PAN shall be mandatory for borrowers and co-borrowers as per Sec 114B of IT act. In the absence of PAN, Form 97 shall be accepted for borrowers and co-borrowers. However, the income validation has to be*

performed in line with income declared in Form 97.

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

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

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 have 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 Limited(VFL)

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 activitiesrelating 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 (VFLs).

a. VFL 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 helps 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

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. In case of a match, the same will be analyzed by AML team to rule out the involvement of terrorist activities by doing an Enhanced Due Diligence.
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, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.

5.1.1 Unique Customer Identification number (UCIC)

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within Veritas. UCIC helps Veritas to identify its customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

- In Veritas, UCIC number is generated for every individual customer at Dedupe stage itself across products. This helps in identifying the customer at pre-onboarding stage.
- If a customer has already been allotted a UCIC, the new account(s) of that customer must be opened under the existing UCIC only. No additional UCIC shall be created by LOS or LMS.

- The Credit team shall evaluate the individual customer for existing UCIC at the loan processing stage or Deduplication stage and confirm.
- A Unique Customer Identification Code (UCIC) will help Veritas to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable Veritas to have a better approach to risk profiling of customers.

5.2)RISK MANAGEMENT

- The Company has put in place appropriate procedures to ensure the 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.

Process of Risk Profiling

For Risk management, the Company has a Risk based approach, after taking into consideration the assessment and risk perception of the Company. Each customer is categorized into low, medium and high risk. In this note, the term "risk" is considered in the context of money laundering and financing terrorism (not credit risk, loan default risk, etc.). Risk profiling of customer is based on customer's identity, social/financial status, nature of business activity and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The Company has adopted the following classification for risk categorizations of its customers.

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 are

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 working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialing (IDD) call service.
2. Companies having close family shareholding or beneficial ownership
3. Non Resident customers where Salary credits are credited to customer's NRI Bank accounts, customers transferring funds through approved money exchangers
4. High net worth Individuals with more than Rs.5 crores
5. Trust/Charities
6. Firms with sleeping partners
7. Money changers

c) High Risk Category

Categorization of high risk shall depend 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. politically exposed persons (PEPs) of Indian/foreign origin,
2. non-face to face customers, and

3. those with dubious reputation as per public information available, etc.
4. NRI Customers' if the customers earn Salary in Cash in origin country or employed in Countries that are classified under FATF which are listed as part of Grey list. However, NRIs from countries listed under Black list shall not be funded.
5. 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.
6. 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.
7. Gambling/gaming including "junket operators" arranging gambling tours.
8. Jewelers and Bullion Dealers.

Process of Risk Categorization

- Relevant section specifying the Risk Category of the customer should be filled in LOS
- Risk categorization of customers into Low, Medium & High Risk shall be done based on information available.
- For customers categorized as "High risk", enhanced due diligence as specified below is mandatory:

EDD includes

1) Since Veritas is into subjective assessment of the customer, the customer's premises /Business place to ascertain the real existence of such a business/industrial unit/financial status person and its scale of operations commensurate with its turnover with higher level of diligence by the employees.

2) Case needs to be approved post recommendation from Business Head by Chief Risk Officer after review of customer visit report, financial documents & source of funds.

3) Operations shall ensure that no disbursement is made unless the Risk Categorization is done.

4) Operations shall also ensure that the respective approvals for customers classified as High-Risk customer are available.

5) Operations to also ensure that correct risk categorization is updated in LOS.

It is to be noted that the customer profile will be a confidential document, and details contained therein shall not be divulged for any other purposes. Adequate care should also be taken by the branch functionaries to seek only such information from the customer, which is relevant to the risk category and is not intrusive.

CDD measures are applied based on the risk profile of the customer. The risk ratings and the related due diligence measures are summarized below:

Risk Profile

1) Low & Medium risk -Standard Measures
2) High risk - Enhanced Due Diligence

CUSTOMER SCREENING

The risk assessment procedure begins with screening of the Negative/ Freeze lists. On receipt of any caution lists being provided by the Reserve Bank of India to the Legal/ Compliance /Secretarial Department, the same shall be provided to the IT department for uploading in Internal Dedupe Database.

The procedure for screening of lists is as follows:

(i) The Internal Dedupe database will be enhanced with various lists to screen the name, date of birth and /or relevant data of the customer,

(ii) When information of an existing customer or the Beneficial Owner of an existing account, subsequently becoming a PEP is obtained either from information available in public domain or customer interaction at branch or during servicing of accounts, senior management approval would be required to continue the business relationship, and the account shall be subject to enhanced CDD measures.

(*-Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.)

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. Passport
2. Voter's Identity Card
3. Driving License
4. Letter issued by National Population Register.
5. Job card issued by NREGA duly signed by State govt officer
6. Proof of possession of Aadhaar (As per UIDAI, AADHAR card can be used as OVD only on masking the number)

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. Registration Certificate
2. Certificate/license issued by the municipal authorities under Shop and Establishment Act.

3. Sales and income tax returns.

4. CST/VAT/ GST certificate (provisional/final).

5. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

6. 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.

7. Utility bills such as electricity, water, and landline telephone bills

8. Telephone/Fax number/E-mail ID;

9. Recent color photograph

10. Registration certificate as a proof of business/activity in the name of the proprietary firm includes "Udyaam 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 not as Identification document but as a

corroborative document

4. Identification information i.e. Any document as mentioned in OVD list along with 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 97 of the trust.

4. Identification information i.e. Any document as mentioned in OVD list along with 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 authorized 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. Any document as mentioned in OVD list along with Permanent Account Number or Form 97 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 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 but can be approved as per internal credit policy approved by board.

G. Client accounts opened by professional intermediaries

Where the transaction is with a professional intermediary who in turn is on behalf of a single client, that client must be identified. The Company shall not open accounts with such

professional intermediaries who are bound by any client confidentiality that prohibits disclosure of client details to the Company

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.

CKYCR

CKYCR is an entity under CERSAI to receive, store, safeguard and retrieve the KYC records in digital form of a customer. CKYCR manages the KYC for Individual and Legal Entities.

- Sharing of information to CKYCR

• Operations team to upload KYC record of customer within 10 days of commencement of an account-based relation such as booking of the contract. Whenever Veritas receives an updated or additional information of the customer as per amended clause 56(j), within 7 days of receipt of data, it has to be uploaded in CKYCR.

- Applicable operational guideline issued by CERSAI for uploading the KYC data shall be followed.
- The KYC of Individual and Legal Entities to be uploaded with CKYCR of the accounts opened on or after 01.04.2017 and 01.04.2021 respectively.
- The KYC Identifier generated by CKYCR to be informed to Individual and Legal Entity as the case may be.
- The CKYCR identifier generated after submission of KYC is required to be communicated to the respective customer.
- Periodical updation of the KYC information / documents received for Individual and Legal Entities to be done for prior to and after the above-mentioned dates.
- During periodic updation, the customers are migrated to current CDD standards (KYC documentation and information).

Use of Information from CKYCR

With an explicit customer consent and submission of KYC Identifier from customer or with the help of acceptable digital solutions, the company shall retrieve the KYC records online/download from CKYCR using KYC Identifier. In such cases customer will not be required to submit KYC / OVD document or information or any other additional identification document or detail, subject to

following conditions:

i. This provision is applicable only for customers falling under Low Risk or Medium Risk category

ii. That there is no change in information (such as identification detail, Address, other personal information) of the customer as existed in CKYCR, and

iii. Address as per application form and CKYC documents is same.

Additionally, wherever Field Investigation is done, Field Investigation should confirm the same address.

iv. Acceptable vintage of CKYC document used shall be defined by Risk Department from time to time.

v. The document should be valid at the time of proposed loan and it should be an acceptable KYC document as per the Policy.

vi. If for any specified reason customer is picked up for additional/enhanced due diligence, then customer Identity and Address shall be verified through appropriate means which may include submission of additional KYC document and personal visit.

vii. In case contact point verification / customer interaction reports that customer address / KYC detail does not match with the downloaded KYC then fresh KYC shall be obtained.

viii. Additionally, in case of Non-Individual customers the following documents are required afresh from customer / digital source –

- Company - Board Resolution, List of Directors, Latest Shareholding pattern, Power of Attorney (if applicable).
- Partnership Firm - Partnership deed/list of partners with profit sharing ratio, Partnership Authority Letter, Power of Attorney (if applicable).
- HUF – HUF Letter.
- Trust, Society etc. - list of members with beneficial interest percentage Resolution as per entity type, Power of Attorney (if applicable)

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Veritas will upload/update the KYC data pertaining to accounts of individual customers and LEs, at the time of periodic updation as specified in paragraph 38 of the Master Direction, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever Veritas obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9(1C) of

the PML Rules, Veritas will within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR.

CKYCR shall thereafter inform electronically to all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of (*Annex to the circular no.* DOR.AML.REC.49/14.01.001/2024-25 *dated November 06, 2024 on amendment to the Master Direction on Know Your Customer (KYC))*

- an existing customer, Veritas will retrieve the updated KYC records from CKYCR and update the KYC record maintained by Veritas.
- Paragraph 56(j) of the Master Direction is amended to read as follows**:**
  For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, Veritas shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–
- (i) there is a change in the information of the customer as existing in the records of CKYCR; or
- (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
- (iii) the validity period of downloaded documents has lapsed; or
- (iv) Veritas considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

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, VFL shall adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

Process for monitoring and reporting of suspicious transactions

1. Raising suspicion When the concerned officer has reason to believe that a transaction is/ may be a suspicious transaction, which may be linked with terrorist activity or money laundering, s/he must flag the issue forthwith to the AML Team. The concerned officer may consider the following for the purpose of flagging such issue:

• Amount involved are related to crimes of money laundering, the financing of terrorism, or the financing of illegal organizations

• Amount involved are intended to be used in an activity related to such crimes.

Currently the deduplication and screening of terrorist lists are automated which will throw alert to the underwriter for his necessary action.

2. Identification and evaluation

Once the issue is flagged, a formal due diligence is to be conducted to evaluate the suspicion, which shall factor all the attributes and nature of the transaction and in terms of volume, track record, time of transaction, KYC records, behavioral patterns, customer due-diligence information etc. Additional details in relation to a customer can be obtained to substantiate further information. Once proper documentation is obtained and if the concerned officer is satisfied, the issue shall be closed and recorded.

Mere presence of an indicator of suspicion does not necessarily always mean that a transaction is suspicious and needs to be reported. When determining whether a transaction is suspicious, consideration to be given to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its due diligence profile. In some cases, patterns of activity or behavior that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another.

In case, the concerned officer is not satisfied, it shall be further evaluated or escalated to next level, and will be taken up to Principal Nodal Officer who can analyze the case/report and issue shall be closed or reported.

3. Reporting of STR

The PNO may record the reasons therein and evaluate on onward reporting to FIU-IND. Once the PNO is satisfied, that the suspicious transaction is valid and reportable, the same is reported to FIU-IND in accordance with the prescribed formats. The fact of furnishing of suspicious transactions shall be strictly kept confidential to ensure that there is no tipping off to the customer at any level.

The periodicity of KYC updation :

Low Risk	**Every Ten years**
Medium Risk	**Every Eight Years**
High Risk	**Every Two Years**

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	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. 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.
c) Additional measures	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 process

	equivalent to that applicable for on-boarding a new customer. 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. 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. 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.

Due Notices to Customer for Periodic Updation of KYC:

Customers shall be informed in advance regarding the requirement to update their Know Your Customer (KYC) details. At least three advance intimations shall be sent to customers before the due date of periodic KYC updation. These shall be communicated at appropriate intervals through available communication channels, with a minimum of one intimation being sent by physical letter.

In cases where customers fail to comply with the KYC updation requirement by the due date, further at least three follow-up reminders shall be sent at appropriate intervals, using available communication modes, including at least one reminder by physical letter.

The following details are to be covered in customer communication:

- Details of contacts/ escalation mechanism for customer to update KYC at Branch/ Area offices, and

- The potential consequences should be communicated to customers appropriately in letter/ any other mode

The issuance of all such intimations and reminders must be appropriately recorded in the system for each customer, ensuring a complete audit trail.

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 Directions as and when Company starts the procedure of onboarding the customers through non-face-to-face mode or V-CIP.

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. Veritas also does an EDD wherever the customer is screened or alerted in a sanction list and the same to be approved by Chief Risk Officer after review of customer visit report, financial documents & source of funds.

Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk. The following are the indicative list where the risk perception of a customer may be considered higher: (i) Customers requesting for frequent change of address/contact details (ii) Sudden significant change in the loan account activity of the customers (iii) Frequent closure and opening of loan accounts by the customers Enhanced due diligence may be in the nature of keeping the account monitored closely for a re categorization of risk, updation of fresh KYC documents, field investigation or visit of the customer etc., which shall form part of the credit policies of the businesses.

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 on 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/willful 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 are 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 areasonable 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 for enhanced 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 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 the recruitment/hiring process of personnel.

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated March 14, 2019 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. Jurisdictions that do not or insufficiently apply the FATF Recommendations (a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account. (b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

12.1 INTERNATIONAL AML, CFT, PROLIFERATION FINANCING AND FINANCIAL SANCTIONS COMPLIANCE

The Company shall comply with applicable Indian laws, rules, regulations, directions and regulatory requirements, including those issued by the Reserve Bank of India. The Company shall also identify and comply with foreign laws and regulatory requirements to the extent applicable to its operations, transactions, counterparties, business relationships, group structure or other relevant jurisdictional connections.

12.1.2 International Standards and Measures

In designing and periodically reviewing its AML/CFT/PF controls, the Company shall have regard to relevant international standards and measures, including:

a. The Financial Action Task Force (FATF) Recommendations, Interpretive Notes and applicable guidance concerning AML, CFT, proliferation financing, risk-based controls, customer due diligence, beneficial ownership, record-keeping and international cooperation.

b. Applicable United Nations Security Council resolutions, sanctions regimes and consolidated designation lists concerning terrorism, terrorist financing, proliferation financing and other relevant threats.

c. Relevant guidance, standards and regulatory publications issued by competent international, national and sectoral authorities, to the extent relevant to the Company's business and risk

exposure.

International standards shall inform the Company's risk management framework but shall not, by themselves, be treated as replacing applicable domestic legislation or as creating a legal obligation where none otherwise applies.

12.1.3 United States Requirements

Where applicable to the Company, its transactions or relevant counterparties, the Company shall assess and comply with relevant United States AML, CFT and sanctions requirements, including:

a. The Bank Secrecy Act, 31 U.S.C. Chapter 53, as amended, and applicable implementing regulations.

b. Sections 1956 and 1957 of Title 18, United States Code, concerning money laundering and certain transactions involving criminal proceeds.

c. Sections 2339A, 2339B and 2339C of Title 18, United States Code, concerning material support for terrorism and terrorist financing.

d. Applicable sanctions laws and regulations administered by the United States Department of the Treasury's Office of Foreign Assets Control (OFAC), including those issued under the International Emergency Economic Powers Act and other applicable statutory authorities.

The Company shall assess potential US sanctions exposure arising from relevant counterparties, transactions, payment channels, currencies, intermediaries and other jurisdictional connections. Applicable prohibitions shall be observed, and potential violations shall be escalated to the Legal and Compliance Departments.

12.1.4 United Kingdom Requirements

Where applicable, the Company shall assess and comply with relevant United Kingdom AML, CFT and sanctions requirements, including:

a. The Proceeds of Crime Act 2002.

b. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended, and applicable regulatory requirements.

c. The Terrorism Act 2000 and other applicable legislation relating to terrorist financing, terrorist property and associated offences.

d. The Sanctions and Anti-Money Laundering Act 2018 and applicable sanctions regulations made thereunder.

The Company shall assess relevant UK jurisdictional exposure, screen relevant parties where appropriate, investigate potential sanctions matches and escalate suspected breaches for legal

assessment and appropriate action.

12.1.5 Other Foreign Jurisdictions

Where the Company's activities, counterparties, transactions, business relationships or other relevant connections create exposure to another jurisdiction, the Legal and Compliance Departments shall assess the applicability of that jurisdiction's AML, CFT, proliferation-financing and financial-sanctions requirements.

The assessment may include, where relevant, the laws and regulations of the European Union and its Member States, Singapore, the United Arab Emirates, Canada, Australia and other jurisdictions in which the Company conducts business or to which its transactions are materially connected.

The Company shall not assume that foreign legislation applies solely because it is listed in this Policy. The applicable requirements, including any licensing, reporting, screening, asset-freezing, transaction-restriction and record-retention obligations, shall be determined on the basis of the relevant law and facts.

12.1.6 Risk Assessment and Customer Due Diligence

The Company shall incorporate relevant international and cross-border ML/TF/PF risks into its existing risk assessment and customer due diligence procedures. As appropriate to the assessed risk, these procedures shall include:

a. Identification and verification of customers, beneficial owners and persons acting on behalf of customers.

b. Assessment of customer, geographic, product, service, delivery-channel, transaction and counterparty risks.

c. Enhanced due diligence for higher-risk relationships, transactions and jurisdictions, where required by applicable law or warranted by the Company's risk assessment.

d. Ongoing monitoring to identify unusual activity, complex transaction structures, possible sanctions evasion and potential links to money laundering, terrorist financing or proliferation financing.

e. Appropriate screening of customers, beneficial owners, connected parties and transactions against applicable sanctions and terrorist-designation lists.

The extent and frequency of these measures shall be proportionate to the identified risk and consistent with applicable legal requirements.

12.1.7 Sanctions Screening, Escalation and Asset Restrictions

The Company shall maintain documented procedures for sanctions screening, identification of potential matches, investigation, escalation, decision-making and record-keeping.

Screening shall include applicable Indian and United Nations designations and other foreign sanctions lists where relevant to the Company's legal obligations or assessed risk exposure. The use of any additional sanctions list shall be governed by a documented assessment of its relevance and legal implications.

Potential matches shall be investigated promptly. Confirmed matches, unresolved material alerts and suspected sanctions breaches shall be escalated to Compliance. Freezing, blocking, rejecting, suspending or otherwise restricting transactions or assets shall be undertaken in accordance with the applicable legal regime and competent-authority directions. No exception or release shall be authorised contrary to applicable law.

12.1.8 Suspicious Activity Reporting and Confidentiality

Employees shall promptly escalate suspected money laundering, terrorist financing, proliferation financing, sanctions evasion and other relevant financial crime concerns in accordance with the Company's internal procedures.

The Principal Officer and relevant Compliance personnel shall assess reporting obligations under applicable Indian law, including requirements relating to FIU-IND, and separately assess any foreign reporting obligations that may apply. A report to one authority shall not be assumed to satisfy a reporting obligation to another authority unless legally established.

The Company shall comply with applicable restrictions on tipping off, confidentiality, disclosure of suspicious activity reports and the handling of sensitive information.

12.1.9 Jurisdictional Applicability Register and Legal Updates

The Risk & Compliance Departments shall maintain a jurisdictional applicability register identifying, as relevant:

a. The jurisdictions and foreign regulatory regimes assessed.

b. The applicable laws, regulations, sanctions regimes and regulatory requirements.

c. The basis for determining applicability or non-applicability.

d. The controls, responsible functions and reporting or escalation requirements arising from the assessment.

e. The date of the latest review and the next review due date.

The register shall be reviewed periodically and when material changes occur in the Company's business, cross-border activities, counterparties, transaction flows, regulatory environment or

applicable sanctions regimes.

12.1.10 Governance, Training and Record-Keeping

The Risk & Compliance Departments shall coordinate implementation of this section with the business functions, operations, and other relevant stakeholders. Employees involved in customer onboarding, credit appraisal, transaction processing, monitoring, sanctions screening and reporting shall receive appropriate role-based training.

The Company shall maintain records of relevant risk assessments, legal applicability decisions, screening results, escalations, approvals, reports and corrective actions in accordance with applicable statutory, regulatory and internal retention requirements.

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

a) Customer Education:

The frontline staff 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 forfrontline 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 theCompany'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 by 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.

d. Applicability to branches and subsidiaries outside India: The Company does not have operations/subsidiaries outside India