

FINALEAP FINSERV PRIVATE LIMITED

KYC POLICY

KYC POLICY

| Sr No. | Particulars | Page No. |
|---------------|--|-----------------|
| 1 | Introduction | 3 |
| 2 | Objectives | 3 |
| 3 | Regulatory Framework | 3 |
| 4 | Definitions | 4 |
| 5 | Key Elements | 6 |
| 6 | Customer Acceptance Policy | 7 |
| 7 | Customer Identification Procedure | 7 |
| 8 | Customer Education | 8 |
| 9 | Monitoring of Transaction | 8 |
| 10 | Money Laundering and Terrorist Financing Risk Assessment | 8 |
| 11 | Risk Management | 9 |
| 12 | Customer Due Diligence Procedure | 11 |
| 13 | Record Keeping | 15 |
| 14 | Enhanced Due Diligence | 16 |
| 15 | Appointment of Designated Director / Principal Officer | 17 |
| 16 | Reporting to Financial Intelligence Unit – India | 17 |
| 17 | General | 18 |

INTRODUCTION

Despite various endeavors, the financial needs of India's micro, small, and medium enterprises (MSME) have remained mostly unmet.

The following KYC & AML policy of Finaleap FinServ Private Limited (hereinafter referred to as 'Company') has been approved by the Board of Directors in accordance with RBI recommendations released from time to time.

This policy applies to the entire range of products and services provided by the Company.

The foregoing guidelines will apply to all Finaleap FinServ Private Limited branches and offices.

OBJECTIVE

In response to the Financial Action Task Force's (FATF) recommendations, the Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all Non-Banking Financial Companies (NBFCs) in the context of Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies. As a result, VFPL has accepted the aforementioned KYC requirements, with appropriate adjustments based on the company's commercial activities. The Company has ensured that a proper policy framework for KYC and AML measures is created in accordance with RBI rules and implemented after being approved by its Board of Directors.

REGULATORY FRAMEWORK

Regulated Entities (REs) are required to follow certain customer identification procedures and monitor their transactions under the provisions of the Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India. REs must take steps to put the requirements of the aforementioned Act and Rules into effect, including any operational instructions issued as a result of the change (s).

The Reserve Bank of India (RBI) has mandated "Anti Money Laundering" guidelines/ standards in Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 and subsequent updates thereto.

The following are the broad objectives:

- a) Prevent NBFCs from being utilised for money laundering by criminal elements, whether purposefully or accidentally.
- b) The guidelines also require the Company to make reasonable efforts to determine the identity and beneficial ownership of accounts, the source of funds, the nature of the customer's business, the reasonableness of account operations in relation to the customer's business, and other factors that aid the Company in risk management.
- c) Implement suitable controls for detecting and reporting suspicious activity in accordance with applicable laws/procedures.

d) To adhere to all applicable rules and regulations.

g) Ensure that all relevant personnel are properly trained in KYC/AML/CFT procedures.

DEFINITIONS

Beneficial Owner (BO)

a. In the case of a firm, the beneficial owner is the natural person(s) who has/have a controlling ownership stake or exert control through other means, whether acting alone or together, or through one or more juridical persons.

For the purposes of this subclause,

1. A "controlling ownership interest" is defined as ownership of/entitlement to more than 25% of the company's shares, capital, or profits.
2. "Control" means the right to choose a majority of directors or to direct management or policy choices, whether through shareholding, management rights, shareholders agreements, or voting agreements.

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

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

Explanation: Societies are included in the term "body of individuals." The beneficial owner is the appropriate natural person who holds the property if no natural person is found under (a), (b), or (c) above.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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.

Customer

Means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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'

Customer identification - means undertaking the process of CDD.

Officially valid document (OVD)

Passport, Driving license, PAN card, Voter ID / Election ID card, Job card issued by NREGA duly signed by an officer of the State Government, and Aadhaar Card / letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Provided that where 'simplified measures' are applied for verifying the identity of the customers the following documents shall be deemed to be OVD:

- i. identity card with applicant's photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- ii. Letter issued by a Gazette officer, with a duly attested photograph of the person.

Provided further that where 'simplified measures' are applied for verifying, for the limited purpose of, proof of address the following additional documents are deemed to be OVDs:

- 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.

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)

KEY ELEMENTS

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

For the purpose of KYC policy, a “customer” will be defined as:

- Any person or entity connected with a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.
- A person or entity that maintains an account and/or has a business relationship with Company.
- The one on whose behalf the account is maintained (i.e., the beneficial owner).
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Company Secretaries, Chartered Accountants, Solicitors etc. as permitted under the law.

CUSTOMER ACCEPTANCE POLICY

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

- No account is opened in anonymous or fictitious/benami name.
- 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.
- No transaction or account-based relationship is undertaken without following the CDD procedure.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
- 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.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- 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.
- The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose.
- The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.

CUSTOMER IDENTIFICATION PROCEDURE

Customer identification means 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.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

Customer Education:

The Company takes adequate measures to educate the customer on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the customers. Wherever we desire to collect any information about the customer for the purpose other than KYC requirement, it will not form part of the loan application. Such information is being collected separately, purely on a voluntary basis in a form prescribed by Company after explaining the objective to the customer and taking the customer's express approval for the specific uses to which such information could be put.

The front desk 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.

MONITORING OF TRANSACTION:

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.

Illustrative list of activities which is construed as suspicious transactions

- 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.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
 - a. 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.
 - b. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
 - c. 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.
- Certain Employees of the Company arousing suspicion:
 - a. An employee whose lavish lifestyle cannot be supported by his or her salary.
 - b. Negligence of employees/willful blindness is reported repeatedly.
- Some examples of suspicious activities/transactions to be monitored by the operating staff:
 - a. Multiple accounts under the same name
 - b. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.
 - c. There are reasonable doubts over the real beneficiary of the loan
 - d. Frequent requests for change of address

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT:

As per the RBI notification on the KYC amendment dated April 20, 2020, the KYC policy of the company includes the amendment with regard to Money Laundering and Terrorist Financing Risk Assessment by the Regulated Entities (REs).

a. REs 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.

mentioned below is in his judgment falling in a different category, he may categorize the customer, so long as appropriate justification is provided in the customer file.

Indicative List of Risk Categorization:

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)

For example People belonging to lower economic strata of the society whose accounts show small balances and low turnover

Medium & High Risk Category

Customers who are likely to pose a higher-than-average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples are:

1. Non-Resident customers
2. High Net worth Individuals
3. Trust, charities, NGO's and Organization receiving donations
4. Companies having close family shareholding or beneficial ownership
5. Firms with 'sleeping partners'
6. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
7. Non-face-to-face customers
8. Those with dubious reputation as per public information available
9. Accounts of bullion dealers and jewelers

CUSTOMER DUE DILIGENCE PROCEDURE:

I. IDENTIFICATION:

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

A. Individual

1. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication)
2. Permanent Account Number (PAN)
3. Passport

4. Voter's Identity Card
5. Driving License
6. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company.

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. Aadhaar Number (where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained. At the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication)
2. Permanent Account Number (PAN)
3. Registration Certificate
4. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
5. Sales and income tax returns.
6. CST/VAT/ GST certificate (provisional/final).
7. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
8. 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.
9. Utility bills such as electricity, water, and landline telephone bills
10. Telephone/Fax number/E-mail ID;
11. Recent color photograph

In cases where the Company is satisfied that it is not possible to furnish two such documents, 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. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
4. Identification information i.e. Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.

D. Partnership Firms

1. Registration certificate

2. Partnership deed
3. Identification information i.e., Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.

1. Registration certificate
2. Trust deed.
3. Identification information i.e., Aadhaar Card and PAN Card in respect of managers, officers or employees holding an attorney to transact on its behalf.

E. Unincorporated association or body of individuals:

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

The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above

1. The Credit Head of Company has the power to approve the following document in lieu of ID and address proof
 - A certificate from the public authority (i.e) Gazette Officer of State or Central Govt., /Magistrate/MRO/VRO/Gram Panchayat Sarpanch/notary public.

In lieu of Identity proof

- Notarized copy of Marriage certificate with the applicant photograph.

In lieu of address proof

- Rental agreement along with rent receipt and utility bill of the Landlord.
 - In case the customer has a temporary address being a transit arrangement provided by real estate builder – Allotment letter issued by the builder plus permanent address proof
 - In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by Close Relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address.
2. The Credit Head of Company jointly with the concerned Sales Head has further delegated the approval powers to accept the above documents to credit managers, as they may deem fit and necessary, in this regard.
 3. In the event of any genuine reason for non-availability of any of the prescribed documents or to approve any deviations for change in the documents prescribed under this policy, the Credit

Head jointly with the Sales Head considers approving any other document not stated above based on the product, market requirements and also on the merits of the case.

II. VERIFICATION

As part of the Credit Policy of the Company, documents and implemented appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. 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.

i. Verification through documents:

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers by the Company as provided in annexure to this policy. These are appropriately covered in the Credit Policy of the Company.

The Company also accepts physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post is also accepted as an 'Officially Valid Document'.

As per RBI instruction the Company also downloads e-Aadhaar from UIDAI website as an officially valid document subject to the following:

- a) If the prospective customer knows only his / her Aadhaar number, the Company needs to print the prospective customer's e-Aadhaar letter in the company directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.
- b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the Company prints the prospective customer's e-Aadhaar letter directly from the UIDAI portal; or adopt e-KYC procedure as mentioned below.

Verification through non-documentary methods:

Indeed, the Company mainly depend upon this method:

1. Contacting or visiting a customer;
2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
3. Checking references with other financial institutions; or
4. Obtaining a financial statement.

ii. Additional verification procedures.

The business process verification procedures of the Company also address the following situations where:

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The sales executive is not familiar with the documents presented;
3. Where the sales executive is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and
4. If the sales executive cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

The Credit Head along with Sales Head, advise the credit managers to make a personal visit to entangle the situation. The Company will not do any transactions with non-face-to-face customers.

RECORD KEEPING

- a. Maintenance of records of transactions:

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

(i) All cash transactions of the value of more than Rs. 2 lacs, though by policy the Company does not accept cash deposits in foreign currency.

(ii) All series of cash transactions integrally connected to each other which have been valued below Rs. 2 lacs where such series of transactions have taken place within a month.

(iii) All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.

(iv) 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; any such transactions;

(v) records pertaining to identification of the customer and his/her address; and (vi) 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

- b. Records to contain the specified information:

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

i. the nature of the transactions;

ii. the amount of the transaction and the currency in which it was denominated; iii. the date on which the transaction was conducted; and iv. the parties to the transaction.

c. 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.

ENHANCED DUE DILIGENCE

The company is primarily engaged in MSME 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. The existing credit policies of the company in respect of its various businesses ensure that the company is not transacting with such high risk customers.

The company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. The company has established appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the company.

The following are the indicative list where the risk perception of a customer which is considered higher:

- i. Customers requesting for frequent change of address/contact details
- ii. Sudden change in the loan account activity of the customers
- iii. Frequent closure and opening of loan accounts by the customers

CIP Notice:

Enhanced due diligence is in the nature of keeping the account monitored closely for a re-categorization of risk, updating of fresh KYC documents, field investigation or visit of the customer, etc., which forms part of the credit policies of the businesses.

The Company shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

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.

Reliance on third party due diligence:

The company shall not on rely on third party due diligence.

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. Shivprasad Kesare, Co-founder and Director will be the Designated Director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Mr. Sachin Kardile 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.

REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA

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

GENERAL

a. Closure of Accounts Closure/Financing Termination/Business Relationship When the Company is unable to implement suitable KYC measures due to the client's failure to provide information and/or cooperation, the Company will terminate the Financing/Business Relationship after giving the customer due notice and explaining the reasons for the decision. This decision must be made with the approval of the key managerial personnel who are authorized to make it.

b. KYC for Existing Accounts: While the KYC guidelines will apply to all new customers, existing clients will be subject to the same requirements based on materiality and risk. Existing client transactions, on the other hand, would be regularly checked for any strange patterns in account operation

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