



BERAR FINANCE LIMITED
POLICY ON KNOW YOUR CUSTOMER (KYC) / ANTI
MONEY LAUNDERING (AML) MEASURES

RECORD OF REVIEW:

Document Number	01
Version Number	09
Document Classification	External
Originally formulated	June 22, 2015
Created by	Compliance Department
Reviewed by	Risk Management Committee
Approved by	Board of Directors of the Company

<u>Version No</u>	<u>Created/Modified Date</u>
1	June 22, 2015
2	March 19 , 2016
3	March 27, 2017
4	May 18, 2018
5	May 19, 2021
6	June 29, 2021
7	April 28, 2022
8	May 30,2023
9	March 27, 2024

Policy on Know Your Customer/Anti-Money Laundering Measures

Table of Contents

Sr. No	Contents	Pg. No.
1	Introduction	4
2	Regulatory Requirement	4
3	Objectives and Scope of Policy	4
4	Applicability	5
5	Definitions	5
6	Compliance of KYC Policy	9
7	Key Elements	9
8	Customer Acceptance Policy (CAP)	9
9	Customer Identification Procedure (CIP)	11
10	Customer Profile	12
11	Customer Education	12
12	Monitoring of Transaction	12
13	Enhanced Due Diligence	16
14	Risk Management	16
15	Money Laundering and Terrorist Financing Risk Management	17
16	Identification	18
17	Verification	18
18	Maintenance of Records of Transactions & Identity	18
19	Preservation of Records	19
20	Central KYC Registry (CKYCR)	20
21	Accounts of Politically Exposed Persons (PEPs)	20
22	Appointment of Designated Director	20
23	Appointment of Principal Officer	21
24	Reporting Requirements to Financial Intelligence Unit – India (FIU-IND)	21
25	Reporting to Financial Intelligence Unit – India	21
26	Confidentiality of Information	22
27	Hiring of Employees and Employee Training	22
28	Investors KYC Policy	22
29	Amendment	23
Annexure I	Indicative list for Risk Categorisation	24
Annexure II	Customer Identification Procedure – KYC documents that may be obtained from borrowers/investors & depositors	25

Policy On Know Your Customer (KYC) / Anti Money Laundering (AML) Measures

1. Introduction

Berar Finance Limited is a Non-Banking Financial Company (“NBFC”) having valid Certificate of Registration no. 13.01109 with Reserve Bank of India (“RBI”) vide registration under current RBI classification as NBFC - Investment and Credit Company (“NBFC-ICC”) – Deposit taking Systemically Important (“ICC-SI”) with more than 30 years of experience in asset finance business.

Founded in 1990, Berar Finance Limited (“BFL”) is one of the oldest vehicle financing NBFCs in Central and West India with a network of 100+ branches across the states of Maharashtra, Chhattisgarh, Madhya Pradesh, Telangana, Gujarat and Karnataka.

We specialize in providing two-wheeler loans, Vehicle Refinance, Four-Wheeler Loans (Used Cars), Personal Loans, Demand Loans and Secured MSME Loan /Loan against Property (LAP) on flexible repayment terms with focus on quick turnaround and customer convenience. Our aim is to partner with our customers in the realization of their ambitions.

2. Regulatory Requirement

The “Know Your Customer” (“KYC”) guidelines issued by the Reserve Bank Of India (“RBI”) (RBI /DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016) as updated from time to time aims at preventing Non-Banking Finance Companies (“NBFCs”) from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism. Accordingly, in compliance with the guidelines issued by RBI regularly, the Policy on Know Your Customer (KYC)/ Anti-Money Laundering (AML) Measures (“Policy”) of Berar Finance Limited (“Company”) is hereby formulated and approved by its Board of Directors (“Board”).

3. Objectives and Scope of Policy

- To prevent criminal elements from using the Company for money laundering activities.
- To lay down explicit criteria for acceptance of customers.
- To establish procedures to verify the bona-fide identification of individuals/ non individuals before becoming an account holder/customer.
- To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.
- In respect of customers and reporting of such transactions.
- To develop measures for conducting due diligence.
- To comply with applicable laws and regulatory guidelines.

4. Applicability

This Policy is applicable to all products offered by the Company and all its offices and branches. This Policy is also applicable to all persons who are acting as agents of the Company.

5. Definitions

- a. **“Aadhaar number”** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
- b. **“Account”** includes Deposits as well as borrowings by and from the Company.
- c. **“Act”** and **“Rules”** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto. Together the Act and the Rules are referred to as PMLA.
- d. **“Beneficial Owner”** in relation to a customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the customer. A list of persons who are to be considered as such BOs in relation to a customer is given below: -

Type of Customer	Persons to be considered Beneficial Owners (BOs)
Public / Private Limited Companies	<ul style="list-style-type: none"> a) A natural person having, whether alone or together, or through one or more juridical person, ownership of or entitlement to more than ten percent of shares or capital or profits of the Company; or b) A natural person having, whether alone or together, or through one or more juridical person, 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 shareholder's agreements or voting agreements; or c) Where none of the above is been identified – a natural person who holds the position of senior managing official.
Partnership Firm	<ul style="list-style-type: none"> a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than ten percent of capital or profits of the partnership; or b) Where the above is not been identified – a natural person who holds the position of senior managing official
Unincorporated association of persons or body of individuals	<ul style="list-style-type: none"> a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than fifteen percent of property or capital or profits of such association or body of individuals; or b) Where the above is not been identified – a natural person who holds the position of senior managing official.
Trust/ Foundation	<ul style="list-style-type: none"> a) The Author of the trust; or b) The Trustees of the trust; or c) The Beneficiaries of the trust with ten percent or more interest in the trust; or d) A natural person exercising ultimate effective control over the trust through a chain of control or ownership.
<p>Exemption from identification of BO: It is not necessary to identify and verify the identity of any shareholder or beneficial owner of an entity where the customer or the owner of the controlling interest is:-</p> <ul style="list-style-type: none"> (i) an entity listed on a stock exchange in India, or (ii) an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such listed entities. 	

- e. **“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.

For the purpose of this Policy, a “customer” will include the following:

A person or entity who is engaged in financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting (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; or

Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company. e.g., a wire transfer or issue of a high value demand draft as a single transaction.

A past as well as prospective customer having attempted or executed transactions.

- f. **“Customer Due Diligence” or “CDD”** means identifying and verifying the Customer and the Beneficial Owner.
- g. **“Customer identification”** means undertaking the process of CDD.
- h. **“Central KYC Records Registry” (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- i. **“Designated Director”** means a person designated by the Regulated Entity to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.
- j. **“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.
- k. **“Money Laundering”** shall have the same meaning as defined under section 3 of the Prevention of Money Laundering Act, 2002.
- l. **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- m. **“Officially Valid Document” (“OVD”)** means means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that
- a) Where the customer submits his/her proof of possession of Aadhaar number as and OVD, he/she may submit in such form as are issued by the Unique Identification Authority of India.
 - b) Where the OVD furnished by the customer does not have update address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
 - Utility bill which is not more than two months old of any service provider (electricity,

- telephone, post-paid mobile phone, piped gas, water bill);
- Property or municipal tax receipt;
 - Pension or family payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;
- c) The customer shall submit OVD with current address with a period of three months of submitting the documents specified as above.
- d) (as and when applicable) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
- n. **“Non-face-to-face customers”** means customers who open accounts without visiting the branch/offices of the Regulated Entity/Entities or meeting the officials of a Regulated Entity.
- o. **“Principal Officer”** means an officer at the management level nominated by the Regulated Entity responsible for furnishing information as per rule 8 of the Rules.
- p. **“Reporting Entity”** for the purpose of this Policy would mean the Company, Berar Finance Limited.
- q. **“Senior Management”** as defined in Nomination and Remuneration Policy of the Company.
- r. **“Suspicious transaction”** means a transaction as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
 - appears to be made in circumstances of unusual or unjustified complexity; or
 - appears to not have economic rationale or bona-fide purpose; or
 - gives rise to a reasonable ground of suspicion that it may involve Terrorist Financing.
- s. **“Transaction”** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes -
- opening of an account;
 - deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
 - the use of a safety deposit box or any other form of safe deposit;
 - entering into any fiduciary relationship;
 - any payment made or received in whole or in part of any contractual or other legal obligation;
 - any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and
 - establishing or creating a legal person or legal arrangement.

- t. **“Terrorist financing”** is the financing of terrorist acts, terrorists and terrorist organisations.
- u. **“Wire Transfer”** for the purpose of this Policy, Wire Transfer and its related definitions would have the same meaning as assigned to it under the RBI’s Guidelines on ‘Know Your Customer’ and Anti-Money Laundering Measures, as amended from time to time.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the RBI Guidelines and other regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6. Compliance of KYC Policy

The Company’s senior management team comprising of respective vertical heads (oversee KYC compliance in line with the Policy. The Internal Audit team shall on a continuous basis conduct an independent evaluation of adherence to KYC compliance requirements and submit audit notes and report on compliance to Audit Committee on quarterly basis. The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

7. Key Elements

KYC procedures also enable the Company to know/understand its Customers and their financial dealings better which in turn help to manage its risks prudently. We have framed the Policy incorporating the following four key elements:

- Customer Acceptance Policy (“CAP”);
- Customer Identification Procedures (“CIP”);
- Monitoring of Transactions; and
- Risk management.

8. Customer Acceptance Policy (“CAP”)

The Company’s CAP lays down criteria for acceptance of customers. The Company will:

- a. Ensure no account is opened in anonymous or fictitious *benami* name(s);
- b. Ascertain the volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk (these customers will require very high level of monitoring).
- c. Ensure documentation requirements and other information collected in respect of different categories of customers (Risk Categorisation as per Annexure I) are commensurate with the perceived risk and keeping in mind the requirements of Act and guidelines issued from time to time by the RBI;
- d. Verify the identity and /or obtain documents required as per the risk categorization and the Company will refuse to process a loan account/accept a deposit where the prospective Customer does not co-operate with the Company in providing these details or where the Company is not sure about the reliability of the data furnished by the prospective Customer;
- e. Take adequate steps to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, sanctioned persons;
- f. Prepare the profile for new and existing Customers which are based on risk

categorization. The customer profile contains information relating to the 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, the seeking of such information will not be intrusive, and the Company will not use such confidential information for cross selling or any other purposes.

- g. Ensure circumstances, in which a Customer is permitted to act on behalf of another person/entity, will be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in a fiduciary capacity.
- h. Conduct necessary checks (e.g. sanctions list issued by RBI), before opening a new account to ensure that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or whose name appear in it .
- i. Assign a Unique Customer Identification Code ("UCIC") while entering relationships with new Customers as also for the existing Customers by the Company. The Company shall apply the customer due diligence ("CDD") procedure at the customer level.
- j. Where Goods and Services Tax (GST) details are obtained, the same shall be verified from the search/verification facility of the issuing authority.
- k. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.
- l. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- m. Due Diligence Procedure of customers should be followed for all the joint account holders, while opening a joint account.

If the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the Customer, it shall either not accept or terminate (in case where customer deliberately evades compliance of KYC norms under this policy after commencement of business relationship) business relationship after issuing due notice to the Customer explaining the reasons for taking such a decision. Such decisions being taken by vertical heads after consulting the Principal Officer.

The intent of the Policy is not to result in denial of financial services to public, 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 Customer.

The Company shall carry out full scale CDD before opening an account.

If the Company is suspicious of money laundering or terrorist financing, and reasonably believes that performing the Customer Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report (STR) to FIU-IND.

9. Customer Identification Procedure (“CIP”)

Customer identification means identifying the Customer and verifying his/her/its identity by using reliable, independent source documents, data or information.

The Company obtains the necessary information to establish the identity of each new Customer, whether regular or occasional and the purpose of the intended nature of relationship. The identification procedure is carried out at different stages, i.e. while establishing a relationship, carrying out a financial transaction or when the Company has a doubt about the authenticity or the adequacy of the previously obtained customer identification data.

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

An effective CIP is an important part of the effort by the Company to know its Customers. The Company’s CIP is integrated into the AML (Anti Money Laundering) program for the Company in terms of the **PMLA**, which contains provisions requiring the business processes to:

- Verify the identity of any Person transacting with the Company to the extent reasonable and practicable;
- Maintain records of the information used to verify a Customer’s identity, including name, address and other identifying information and
- Consult Sanctions Lists/ Financial Actions Task Force (“**FATF**”) /Office of Foreign Control Assets (“**OFAC**”) databases for known or suspected terrorists or terrorist organizations / jurisdictions and countries that do not or insufficiently apply the FATF recommendations as provided to the Company by RBI or any other applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.
- The Company shall carry out the customer identification procedures as specified by the Reserve Bank of India in its Master Direction (KYC), 2016 (DBR.AM.BC.81/14.01.001/2015-16 dated 25.02.2016) as amended from time to time.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its Customers that is reasonably designed to know and verify their true identity 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 will carry out ‘Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment’ exercise periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc. The internal risk assessment carried out by the Company should be commensurate to its size, geographical presence, complexity of activities/structure, etc. and shall apply a Risk Based Approach for mitigation and management of the identified risks.

The risk assessment processes shall be reviewed periodically to ensure its robustness and effectiveness.

10. Customer Profile

For the purpose of exercising due diligence on individual transactions in accounts, a 'Customer Profile' of individual Customers is included in the loan application or deposit opening form. The customer profile will contain information relating to the Customer's identity, social/ financial status, information about the Customer's clients' business and their location etc. The information will be of two types namely mandatory and optional as stated below:

(a) Mandatory Information:

(i) Identity (ii) Address (iii) Occupation (iv) Source of funds (v) Monthly Income (vi) Annual turnover (vii) Date of Birth (viii) Dealings with other banks (ix) Assets (approximate value).

(b) Optional Information:

(i) Marital Status; (ii) Educational Qualification; (iii) Details of spouse; (iv) Details regarding children; (v) Other Information which can include queries on a) Car/two-wheeler ownership, b) has a credit card c) has an insurance policy.

The Company shall, where its Customer submits a proof of possession of Aadhaar Card containing Aadhaar Number, ensure redacts or blacks out of his Aadhaar number is done through appropriate means.

11. Customer Education

The Company will take adequate measures to educate the Customers on the objectives of the KYC programme, especially at the time of obtaining sensitive or personal information from the Customers. When required to collect any information about the Customer for the purpose other than KYC requirement, it will not form part of the loan application or deposit opening. Such information will be collected separately, purely on a voluntary basis in a form prescribed by the 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 used. The customer servicing staff is 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 or deposit accounts to public.

12. Monitoring of Transactions

Ongoing Due Diligence

Ongoing monitoring is an essential element of effective KYC procedures. The Company effectively controls and reduces the risk through understanding of the normal and reasonable activity of the Customer and by it having 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 company 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 will be subjected to intensify monitoring.

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/provide insufficient/suspicious information:
- 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.
 - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
- Certain employees of the Company arousing suspicion:
 - An employee whose lifestyle is beyond his/her economic means
 - Negligence of employees/willful blindness is reported repeatedly.
- Multiple accounts under the same name.
- Refusal to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.
- There are reasonable doubts over the real beneficiary of the loan.
- Frequent requests for change of address.

The company may adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

Review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation shall not be less than once in ten years in case of low risk category customers, not be less than once in five years in case of medium risk category customers and not less than once in two years in case of high risk categories in the following manner. The Company shall ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk.

<p>1. INDIVIDUAL CUSTOMERS</p> <p>a) No change in KYC information</p> <p>b) Change in address</p>	<p>A self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.</p> <p>A self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital</p>
---	--

<p>c) Accounts of customers who were minor at the time of opening account on their becoming major</p> <p>d) Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode</p>	<p>channels (such as online banking / internet banking, 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 address, declared by the customer at the time of periodic updation.</p> <p>A fresh photograph shall be obtained from the customer on their becoming a major and it shall be ensured that CDD documents as per the current CDD standards are available with the Company. The Company may also carry out fresh KYC of such customers, wherever required.</p> <p>Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud. The specific conditions stipulated for opening of an account using Aadhaar OTP in non-face-to-face mode under RBI guidelines are not applicable for updation/ periodic updation of KYC.</p>
<p>2. CUSTOMERS OTHER THAN INDIVIDUALS (LEGAL ENTITY)</p> <p>a) No change in KYC information</p> <p>b) Change in KYC information</p>	<p>A self-declaration shall be obtained from the Legal Entity (LE) customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. The Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.</p> <p>The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.</p>

<p>3. ADDITIONAL MEASURES</p>	<p>a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.</p> <p>b) Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.</p> <p>c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self- declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.</p> <p>d) In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.</p> <p>e) The Company shall adopt a risk based approach with respect to periodic updation of KYC.</p>
<p>4. OBLIGATIONS OF CUSTOMERS:</p>	<p>The Customers are required to submit the updated KYC documents to the Company, in case of any updation in the KYC already submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, within a period of 30 days from such update in order to comply with the PML Rules.</p>

13. Enhanced Due Diligence

Enhanced Due Diligence will involve closely monitoring the account, frequently updating KYC documents, field investigation or visiting the customer, etc., which forms part of the credit policies of the businesses.

if the Company has Customers or accounts that are determined to pose a potential high risk including but not limited to non-face to face customers and thereby warrant enhanced scrutiny then it shall conduct Enhanced Due Diligence in connection with such Customers. 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 as per the procedures stipulated by Reserve Bank of India in Master Direction (KYC), 2016 (DBR.AM.BC.81/14.01.001/2015-16 dated 25.02.2016) as amended from time to time.

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

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

In case of sale of repossessed vehicles by company to purchasers/brokers, company shall ensure to collect the KYC (Identity & address proof) so as to ensure the real identity of the buyer of such repossessed vehicles. Company shall obtain a declaration from the buyer that vehicles are being sold by the Company on 'As is Where Is' basis and the buyer is responsible to ensure the name transfer in RTO Records and deletion of the Company's hypothecation thereon. This ensures Company / its original customers is not accountable for repossessed vehicles being used for terrorist or any other unlawful activities.

The Company obtains End Use Declaration letter from customers confirming the purpose of finance taken and a declaration that the Facility shall not be used for any illegal and /or anti-social and / or speculative purposes including but not limited to participation in stock markets / IPOs.

14. Risk Management

- a. The Board of Directors ("Board") of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles and principles for risk categorization of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.
- b. The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new

customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

- c. The Company shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, geographical risk covering customers as well as transactions, type of services offered, delivery channel used for delivery of services, types of transaction undertaken - cash, cheque/monetary instruments, wire transfers, forex transactions etc. The nature and extent of due diligence shall depend on the risk perceived by the Company.
- d. For the purpose of risk categorization, 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, shall be categorized as low risk. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer, are to be met. Customers that are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds, his client profile, geographical risk, type of services offered, delivery channel used for delivery of services, types of transaction undertaken - cash, cheque/monetary instruments, wire transfers, forex transactions etc. The Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.
- e. The various information so collected from different category of customers for the purpose of risk categorization and related to perceived risk shall be on non-intrusive basis, notwithstanding the need for availability of minimum required information to meet the regulatory requirements.
- f. An indicative categorization for guidance is provided in **Annexure I**.

15. Money Laundering and Terrorist Financing Risk Assessment

- a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise regularly to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk.
- b. The assessment process shall 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, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.
- c. The risk assessment by the Company shall be properly documented and be commensurate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.
- d. The outcome of the exercise shall be put up to the Risk Management Committee on a quarterly basis and will be available to competent authorities and self-regulating bodies.
- e. The Company shall apply a Risk Based Approach ("**RBA**") for mitigation and management of the identified risk and should have Board approved policies, controls

and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

16. Identification

All customers shall be identified by a unique identification code. This unique code will be employed to track the facilities availed, monitor financial transactions which assists in risk profiling of customers. The customer identification requirement applicable to borrowers / investors and depositors are detailed in Annexure II to this policy

17. Verification

As a part of the Lending Policy the Company documents and implemented appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the identity of its Customers (Borrower's). 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, non-documentary verification methods or *additional verification procedures* that are appropriate with the associated risks, which are explained below;

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 the Lending Policy. The customer identification requirement applicable to borrowers / investors and depositors are detailed in Annexure II to this policy

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 OVD.

II. Verification through non-documentary methods:

The Company depends on other methods of verification as listed below:

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; or
3. Checking references with other financial institutions.

III. Additional verification procedures.

The Business Head advises the credit team to make a personal visit to address under the following situations.

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 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, to verify the customer's identity.

18. Maintenance of Records of Transactions & Identity

The Company has a system of maintaining proper record of transactions prescribed under

Rule 3, of the PML Rules 2005 and value of transactions, the procedure and manner of maintaining and verification and maintenance of records of the identity of the clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, as mentioned below:

- All cash transactions of the value of more than Rupees Ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below Rupees Ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten lakhs;
- 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
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- As per the RBI guidelines, the Company maintains the following information in respect of transactions referred to in Rule 3 of the Rules:
 - Nature of the transactions;
 - Amount of the transaction and the mode adopted for undertaking the transaction;
 - Date on which the transaction was conducted; and
 - Parties to the transaction.

19. Preservation of Records

The Company will maintain the records containing information of all transactions including the records of transactions detailed in PML Rule 3. The Company should also take appropriate steps to evolve a system **including establishment of appropriate AML / CFT Cell at HO Level** 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 should maintain records relating to the transactions, whether attempted or executed, in such manner & for such period as specified under section 12 of the Prevention of Money Laundering Act, 2002.

The Company should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules. The identification records and transaction data **including attempted & executed** should be made available to the competent authorities upon request.

The Company should ensure that if its customer is a non-profit organization, it shall be registered on the DARPAN Portal of NITI Aayog. If it's not registered, then Company shall take appropriate steps to register the same and maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

20. Central KYC Registry (“CKYCR”)

The Company will ensure that the Customer KYC information is shared with the CKYCR in the manner mentioned in the RBI Directions in RBI’s KYC templates prepared for ‘Individuals’ and ‘Legal Entities’ with Central Registry of Securitization Asset Reconstruction and Security Interest of India (“CERSAI”).

As per the directions NBFCs shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

21. Accounts of Politically Exposed Persons (PEPs)

- A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:
1. The Company have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
 2. Reasonable measures are taken by the Company for establishing the source of funds / wealth;
 3. The approval to open an account for a PEP shall be obtained from the Senior Management;
 4. All such accounts are subjected to enhanced monitoring on an on-going basis;
 5. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Senior Management’s approval is obtained to continue the business relationship;
- B. These instructions shall also be applicable to family members or close associates of PEPs.

Explanation: For the purpose of this Section, “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.

22. Appointment of Designated Director

The Managing Director of the Company has been appointed as Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and Rules.

The Company shall submit the name, designation, address and contact details of the Designated Director to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

23. Appointment of Principal Officer

The Chief Financial Officer has been appointed as Principal Officer of the Company, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under PML Act/ KYC Policy.

The Company shall submit the name, designation, address and contact details of the Principal Officer to the FIU-IND and Reserve Bank of India (RBI), whenever there is any change.

24. Reporting Requirements to Financial Intelligence Unit - India (FIU-IND)

The Company shall furnish the following reports to the Financial Intelligence Unit-India (FIU-IND), with regard to information referred to in Rule 3 of the Rules and in terms of Rule 7 thereof in the manner so specified and within the timelines prescribed therein;

- a. Cash Transactions Report (“CTR”)
- b. Suspicious Transactions Report (“STR”)
- c. Counterfeit Currency Reports (“CCR”)
- d. Non-Profit Organisation Reports (“NPR”)

The Company is registered with FIU-IND with registration number of FI00000735. The Company submits CTR monthly and STR on identification of such transaction with FIU-IND.

The Company has implemented a system not to accept cash of more than Rs. 2 lakhs at a time from its borrowers. Hence, it normally does not and would not have large cash transactions. However, when cash transactions monthly aggregating of more than Rs. 10 lakhs and above are undertaken, the Company will maintain record of all such cash transactions in a separate register at its corporate office.

The Company monitors transactions of a suspicious nature on an ongoing basis for the purpose of reporting it to the appropriate authorities. The extent of monitoring by the

Company depends on the risk sensitivity of the account and special attention is given to all complex unusually large transactions, which have no apparent economic or lawful purpose. The Company shall promptly report such high value cash transactions or transactions of a suspicious nature to the appropriate regulatory and investigating authorities. The Company has a system which alerts inconsistent transactions and profile of the customers is updated for effective identification and reports of suspicious transactions.

25. Reporting to Financial Intelligence Unit – India

The Company should ensure that if its customer is a non-profit organization, it shall be registered on the DARPAN Portal of NITI Aayog. If it's not registered, then Company shall take appropriate steps to register the same and maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

In terms of the PMLA rules, the Company will report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address and portal	
Address	Portal
Financial Intelligence Unit - India 6th Floor, Tower-2, Jeevan Bharati Building, Connaught Place, New Delhi-110001, INDIA Telephone : 91-11-23314429, 23314459	http://fiuindia.gov.in/

The above guidelines do not require the company to report NIL transactions.

26. Confidentiality of Information

Information collected from Customers for the purpose of opening of account shall be treated as confidential and in accordance with the agreement/terms and conditions signed by the Customers. The information collected from Customers shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the Customer. While considering the requests for data/information from Government and other agencies, the Company shall satisfy that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in their transactions.

The exceptions to the said rule shall be as under:

- a) Where disclosure is required under law;
- b) Where there is a duty to the public to disclose such information ;
- c) Such disclosure is required in the interest of the Company; and
- d) Where the disclosure is made with the express or implied consent of the Customer.

27. Hiring of Employees and Employee Training

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

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

28. Investor KYC Policy

The Company's guidelines pertaining to four Key elements viz. customer acceptance policy, customer identification procedures, monitoring of transactions and risk management of this KYC framework, mentioned in this Policy will be equally applicable for its Investors with suitable modifications depending upon the activity undertaken. The Company shall ensure that a proper framework on KYC and anti-money laundering standards are put in place in this regard. Basic KYC shall be completed through details like Certificate of Incorporation, PAN, TIN, GST etc. All funding proposals will be subject to proper checks on OFAC/ FATF / UN Sanctions List circulated by RBI / List of Willful defaulters / Other List of Terrorist Organizations.

The FATF periodically identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT) in its following publications:

- a) High-Risk Jurisdictions subject to a Call for Action, and
- b) Jurisdictions under Increased Monitoring.

In compliance of RBI's Circular regarding Investment in NBFCs from FATF non-compliant jurisdictions dated February 12, 2021, the Company promotes investments from FATF compliant jurisdiction, i.e. from entities whose name does not appear in the aforementioned lists. Records of such checks shall be maintained.

29. Amendment

The Board reserves the right to amend (either in whole or in part), suspend or rescind this Policy at any time. However, no such amendment or modification will be binding on the Employees and Directors unless the same is notified to all in writing or placed on the Company's website. Whilst, the Company has made best efforts to define detailed procedures for implementation of this Policy, there may be occasions when certain matters are not addressed or there may be ambiguity in the procedures. Such instances or ambiguities will be resolved in line with the broad intent of the Policy. The Company may also establish further rules and procedures, from time to time, to give effect to the intent of this Policy and further the objective of good corporate governance. The Board shall also review this policy on a periodic basis and at least once every year.

Annexure I

Indicative list for Risk Categorization:

Sr. No.	Low Risk (Level 1)	Medium Risk (Level 2)	High Risk (Level 3)
1.	Students, Housewives, Pensioners.	Non-Banking Financial Institutions.	Politically Exposed Persons & their relatives.
2.	Salaried Persons	Credit Co-Operative Societies	Jewelers & Bullion Dealers
3.	No frill accounts	Non-Scheduled UCBs	Accounts of construction & real estate dealers & brokers
4.	Shareholders of the company	Travel Agents	Trusts / NGOs / Organizations receiving donations
5.	Small Traders	Dealers in Pharmaceuticals	Persons with dubious reputation, knowledge of which is available in public domain
6.	Self-Employed	Dealers of Wholesale electronic materials	Accounts, being subject to investigation by law enforcement agencies.
7.	Self Help Groups	Advocates, Solicitors & Notaries	Names 100% matching with the persons notified by UNSC.
8.	Staff & their relative accounts	Dormant accounts above ₹10,000.00	Persons with criminal background, knowledge of which is available in public domain.
9.	Co-Operative Housing Societies	Used car sellers	Dealers in antiques
10.	Professionals such as CA, CS, CMA, Doctors, Engineers, Consultants	Dot Com Companies or internet service providers	Dealers in arms
11.	Agricultural & allied activities	Auctioneers	Share brokers
12.	Small Accounts	Restaurants & Bar	NRE / NRO Accounts
13.	Dormant accounts having exposure below ₹ 10,000.00	Telemarketers & Telecommunication service providers	Money Changes / Remitters
14.		Internet Café	New opened accounts for first 6 months
15.		IDD Call Service Providers	KYC Non-Compliant Accounts
16.			Non Face to Face Customers (Eg. POA Accounts & Minor Accounts)
17.			Firms with sleeping partners
18.			HNI Customers
19.			Customers appearing to be Multi-Level Marketing Companies
20.			Clients managed by professional service providers such as law firms, accountants, brokers, etc.

Annexure II

Customer Identification Procedure – KYC documents that may be obtained from borrowers/investors & depositors:

Nature of customer	List of applicable documents
Individual	<p>The Company shall obtain the following from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:</p> <ol style="list-style-type: none"> a) a certified copy of any OVD containing details of his identity and address; and b) the Permanent Account Number (PAN) or Form no.60; and c) One recent photograph d) Such other documents as specified by the Company from time to time. e) the KYC Identifier with an explicit consent to download records from CKYCR. <p>List of OVDs:</p> <ol style="list-style-type: none"> i) Passport, ii) Driving license iii) Proof of possession of Aadhaar number iv) Voter's identity card issued by the Election Commission of India v) Job card issued by NREGA duly signed by an officer of the State Govt. vi) Letter issued by the National Population Register containing details of name and address. <p>Provided that:</p> <ol style="list-style-type: none"> 1) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the UIDAI. 2) where 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:- <ol style="list-style-type: none"> 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) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv) letter of allotment of accommodation from employer issued by State Govt. or Central Govt. Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation. <p>The Credit Head of The Company has the power to approve the following documents in lieu of ID and address proof.</p> <p>In lieu of Identity proof</p> <p>✓ Notarized copy of Marriage certificate with the applicant photograph.</p> <p>Explanation: A document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by</p>

	<p>a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name</p> <p>In lieu of address proof</p> <ul style="list-style-type: none"> ✓ 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 + permanent address proof ✓ In deserving cases where there is no address proof for one of the applicants or guarantors, an affidavit signed by a close relative (only in case of spouse, parents or children) confirming that the co applicant / guarantor is staying together in the same address. <p>3. The Credit Head of The 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.</p> <p>4. 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.</p> <p>Identification number:</p> <p>1. A taxpayer identification number; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAAR number; or number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise;</p> <p>2. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but business process has implemented procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period before disbursement of loan.</p> <p><i>The Company also ensures that all the customers namely applicant, co applicants and guarantor has valid ID proof as prescribed above</i></p> <p>1. The Credit Head of The Company has the power to approve the following document in lieu of ID and address proof</p> <ul style="list-style-type: none"> ✓ <i>A Certificate from the public authority (i.e) Gazette Officer of State or Central Govt./Magistrate/MRO/VRO/Gram Panchayat Sarpanch/notary public.</i>
Companies	<ol style="list-style-type: none"> 1. Certificate of Incorporation, Memorandum of Association and Articles of Association 2. Resolution of the Board of Directors to open an account and identification of those who have the authority to operate the account.

	<ol style="list-style-type: none"> 3. Power of Attorney granted to its managers, officers or employees to transact business on its behalf 4. PAN Allotment Letter 5. Telephone Bill 6. GST number 7. Names of the relevant persons holding senior management position 8. The registered office and principal place of its business, if it is different
Partnership Firms/LLPs	<ol style="list-style-type: none"> 1. Registration Certificate if the partnership deed is registered 2. Address of the registered office and principal place of its business, if it is different 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4. Any official valid documents identifying the partners and the persons holding the power of attorney and their addresses 5. Telephone bill in the name of firm/partners Accounts 6. PAN 7. GST number(if any)
Proprietary Concerns	<ol style="list-style-type: none"> 1. Proof of the name, address and activity of the concern like registration certificate (in case of a registered concern) including Udyam Registration Certificate (URC) issued by Government. 2. Certificate issued by the Municipal authorities under the Shops and Establishment Act, GST returns, Income Tax returns, GST Certificate, Registration documents issued by GST, Professional Tax Authorities, Certificate of Practice issued by Food and Drug Control Authorities etc. 3. Any registration documents issued in the name of the proprietary concern by the central government, state government. We also accept IEC (import-export code issued to the proprietary concern by the office of DGFT as an identity document for opening of account. 4. Income Tax return copy in the name of the sole proprietor where the firm's income is reflected duly authenticated by the Income Tax Authorities 5. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern <p>Any two of the above documents would suffice. These documents should be in the name of the proprietary concern</p>
Trusts, foundations and society	<ol style="list-style-type: none"> 1. Names of trustees, settlers, beneficiaries and signatories. 2. Names and addresses of the founder, the managers/ directors and the beneficiaries. Telephone/fax numbers 3. Names of beneficial owners 4. Certificate of registration, if registered, Trust Deed, PAN or Form 60 of the Trust, Power of Attorney granted to transact business on its behalf. 5. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney,

	<p>founders/managers/ directors and their addresses.</p> <ol style="list-style-type: none">6. Resolution of the managing body of the foundation/ association.7. Telephone bill8. the names of the beneficiaries, trustees, settlor and authors of the trust9. the address of the registered office of the trust; and10. list of trustees and documents, for those discharging role as trustee and authorized to transact on behalf of the trust11. Satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.
--	--