VERSION CONTROL:

Version	Date of Adoption	Change Reference	Owner	Custodian	Approving Authority
1.0	16-Apr-2014	Know Your Customer (KYC) Policy and Anti-Money Laundering (AML) Measures drafted and approved by the Board	Compliance	Compliance	Board of Directors
1.1	08-May-2019	KYC Policy and AML Measures reviewed and updated as per Master Directions of RBI	Compliance	Compliance	Board of Directors

Preamble:

The Reserve Bank of India (RBI) has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML)/Combating Financing of Terrorism (CFT) measures and has advised all NBFCs to ensure that a proper policy framework on KYC and AML/CFT measures be formulated and out in place with the approval of the Board.

The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risk prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company.

Definition:

a. **Customer:** A 'Customer' is defined as hereunder:
   - A person or entity that maintains an account and/or has a business relationship with the Company;
   - One on whose behalf such relationship is maintained (i.e. beneficial owner)
   - Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law; and
   - Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company, say a wire transfer or issue of a high value demand draft as a single transaction.

b. **Person:** A 'Person' shall have the meaning as defined under KYC policy of RBI (and any amendment from time to time by RBI) which at present is as follows:
   'Person' shall include:
   - an Individual;
   - a Hindu Undivided Family;
   - a Company;
   - a Trust
   - a Firm;
   - an association of persons or a body of individuals, whether incorporated or not;
   - every artificial juridical person, not falling within any one of the above person (a to e);
   - any agency, office or branch owned or controlled by any one of the above persons (a to f).

c. **Politically Exposed Persons (PEPs):** Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, Senior Politicians, Senior Government /judicial /military

officers, Senior executives of State-Owned Corporations, Important political party officials, etc. Company should gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Company should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.

Objectives, Scope and Application of the Policy:

The primary objective is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities.

- To lay down explicit criteria for acceptance of customers.
- To establish procedures to verify the bona-fide identification of individuals/non- individuals for opening of account.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

To fulfil the scope, the Company hereunder framing KYC Policy incorporating the following four key elements:

1. Customer Acceptance Policy;
2. Customer Identification Procedures;
3. Monitoring of Transactions;
4. Risk Management.

1. Customer Acceptance Policy:

The Customer Acceptance Policy (CAP) is developed laying down explicit criteria for acceptance of customers. The CAP shall ensure that explicit guidelines are in place on the following aspects of customer relationship in the Company:

a. Company shall not open any account in anonymous or fictitious / benami name(s) and where proper due diligence cannot be applied.
b. Parameters of risk perception shall be clearly defined in terms of the location of customer and his clients and mode of payments, volume of turnover, social and financial status, etc. to enable categorisation of customers into low, medium and high risk; customers requiring very high level of monitoring, e.g. Politically Exposed Persons shall be, categorised unfailingly in the high risk category. The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category - customer background, country of origin, sources of fund, banking experience and conduct, repayment track record of other lending, CIBIL check, availability of satisfactory financial records. For the purpose of risk categorisation of customer, Company shall obtain the relevant information from the customer at the time of account opening. The Company shall accept customers after verifying their identity as laid down in customer identification procedures. Parameters of risk perception shall be clearly defined in terms of the location of customer and his clients and mode of payments. While carrying out due diligence the Company will ensure that the procedure adopted will not result in denial of services to the genuine customers;

c. The Company should ensure that documents and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002 (Central Act No. 15 of 2003) (hereinafter referred to as PMLA), rules framed there under and guidelines issued from time to time;
d. Not to open an account where the Company is unable to apply appropriate customer due diligence measures, i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non- cooperation of the customer or non reliability of the data/information furnished to the Company. It shall, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
e. Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall 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 shall be opened by an intermediary in a fiduciary capacity; and
f. Necessary checks before opening a new account so as 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, caution list circulated by Reserve Bank of India, from time to time, etc.

The Company shall prepare a profile for each new customer based on risk categorisation. The customer profile shall contain 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, while preparing customer profile the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with her/his consent and after opening the account.

For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk. Illustrative examples of low risk customers would be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies, etc. In such cases, the policy shall 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 shall be categorised 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. The Company shall 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. Examples of customers requiring higher due diligence shall include:

- non-resident customers;
- high net worth individuals:

- trusts, charities, NGOs and organizations receiving donations;
- companies having close family shareholding or beneficial ownership;
- firms with 'sleeping partners';
- politically exposed persons (PEPs) of foreign origin;
- non-face to face customers; and
- those with dubious reputation as per public information available, etc.

As regards the accounts of PEPs, in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company shall obtain senior management approval in such cases to continue the business relationship with such person, and also undertake enhanced monitoring.

The adoption of Customer Acceptance Policy and its implementation shall not become too restrictive and shall not result in denial of the Company's services to general public, especially to those, who are financially or socially disadvantaged.

2. Customer Identification Procedure ("CIP"):

Customer identification means identifying the customer and verifying her / his / its identity by using reliable, independent source documents, data or information while establishing a relationship. As per Rule 9 of the Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

a. at the time of commencement of an account–based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship; and
b. in all other cases, verify identity while carrying out:
    i. transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or
    ii. any international money transfer operations.

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The Company shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

The Company gets sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Rule 9 of the PML Rules provides for the documents/information to be obtained for identifying various types of customers i.e. individuals, companies, partnership firms, trusts, unincorporated association or a body of individuals and juridical persons. The Company taking note of the provisions of the above rule and shall ensure compliance. An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the **Annexure-1**. The internal guidelines based on the experience of dealing with such persons/entities, normal prudence and the legal requirements will also be considered.

Original Seen and Verified (OSV) Norms:
KYC documents provided by the customer (for applicant/co-applicant /guarantor and other related parties) will be sighted in original and verified by the Company's Employee/Sourcing Channel Partner who is authorized to do OSV and signed with "Original Seen and Verified" stamp.

Risk based approach is considered necessary to avoid disproportionate cost to the Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the Company will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall:

a. verify the legal status of the legal person / entity through proper and relevant documents
b. verify that any person purporting to act on behalf of the legal person / entity is so authorized and identify and verify the identity of that person; and
c. understands the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lenders prudence and the legal requirements as per established practices. In case, customer is permitted to act on behalf of another person/entity, the same would be allowed only in conformity with established law and practices and after taking necessary safeguards such as notarizing the Power of Attorney or the mandate, KYC of both the customers and the authority operating the account including the intermediary acting in fiduciary capacity. The Company will take reasonable measures to identify the beneficial owner(s) and verify her/his/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

The document requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

Customer Identification Procedure shall be carried out at different stages i.e.:

- While establishing a business relationship (or)
- Carrying out a financial transaction (or)
- Where the Company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any (or)
- When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

No deviations or exemptions shall normally be permitted in the documents specified for account opening. In case of any extreme cases of exceptions, concurrence of Policy section shall be obtained duly recording the reasons for the same. Suitable operating guidelines for implementation of the KYC/AML guidelines shall be issued by the Company for its different business segments.

The Client Identification Programme is formulated and implemented to determine the true identity of its client keeping the above in view.

Important: Company shall periodically review the risk categorization of loan assets, which shall not be less than once every 6 months. Company will also periodically update the customer identification data (including photograph/s) after the loan account is opened. The periodicity of such updation shall not be less than once in five years in case of low risk category customers; not less than once in two years in case of medium risk category customers and not less than once in annual in case of high risk category customers.

3. Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. The Company can effectively control and reduce their risk only if they have 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 attached with the client. The Company pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Company shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

Background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors shall determine the extent of monitoring. Higher risk accounts shall be subjected to intensify monitoring. Company shall carry out the periodic review of risk categorization of transactions/customers and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

Company shall explore the possibility of validating the new accounts opening application with various watch lists available in public domain, including RBI watch list. After due diligence, any transactions of suspicious nature will be duly reported by principal officer to Director, Financial Intelligence Unit- India (FIU_IND).

To ensure monitoring and reporting of all transactions and sharing of information as required under the law for KYC, the Board may nominate any Director or authorized CMD or any other officer(s) duly authorized by CMD to be designated as Company's Principal Officer with respect to KYC/ AML/ CFT.

Principal Officers for KYC/ AML/ CFT:

Principal Officer(s) for KYC will act independently and report directly to the concerned Director/MD or to the Board of Directors. The role and responsibilities of the Principal Officer(s) should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued

from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

The collection of data on the borrower side would be the primary responsibility of Relationship and CMOG team and the required data as per formats (Company Application Form) prescribed in this policy shall be collected, irrespective whether Company is the lead institution or there are other co-financing institutions. To ensure monitoring of the KYC Guidelines laid down by Company, the borrowers may be requested to resubmit their forms annually or in case there is any change in the structure of entity within15 days of information of such change.

4. Risk Management:

The Board of Directors of the Company will ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will 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 the Board, devise procedures for creating Risk Profiles 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.
The Company's internal audit and compliance functions shall have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function shall provide an independent evaluation of the Companies own policies and procedures including legal and regulatory requirements. The Company ensures that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures.

Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Audit Committee of the Board at quarterly intervals. The Company shall ensure that there is proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

The Company will have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements will 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.

<u>Risk Management Committee ("RMC"):</u>
The Principal officer may submit the periodic report to RMC if a need arises in case of high-risk cases and which may require further guidance from Committee so they can assess the risk involved in the case of different customers on the basis of data collected by the business team. Depending on the requirement, services of an independent consultant having knowledge and background on the subject may be taken. Such issues of categorization shall be kept confidential and shall not be divulged to any third party irrespective of their relationship with Company at any level of organization.

Closure of Accounts/Termination of Financing/Business Relationship:

Where Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the customer, the Company shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Managing Director or Principal Officer.

Maintenance of records of transactions:

The Company will maintain proper record of transactions as required under section 12 of the PMLA read with Rule 3 of the PML Rules, as mentioned below:

a. all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
b. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh 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 lakh;
c. all transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
d. 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 or a document has taken place facilitating the transactions; and
e. all suspicious transactions whether or not made in cash and as mentioned in RBI guidelines / circulars / PMLA rules.

The Company will ensure that its branches continue to maintain proper record of all cash transactions of Rs.10 lakh and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling / head office on a fortnightly basis.

Information to be preserved:

The Company will maintain the following information in respect of transactions as referred to in the preceding point on "Maintenance of Records of Transactions:

a. The nature of the transactions;
b. The amount of the transaction and the currency in which it was denominated;
c. The date on which the transaction was conducted; and
d. The parties to the transaction.

As per Section 12 of PMLA, the Company will maintain records as under:

a. records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules shall be maintained for a period of ten years from the date of transactions between the customers and the Company.
b. records of the identity of all customers of the Company shall be maintained for a period of ten years from the date of cessation of transactions between the customers and Company.

The Company will take steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

Reporting to Financial Intelligence Unit – India

The Company will report information of transaction referred to in clause (a) of sub-section (1) of section 12 of PMLA read with Rule 3 of the PML Rules relating to cash and suspicious transactions, etc., to the Director, Financial Intelligence Unit-India (FIU-IND). The Principal officer shall furnish information, where the principal officer of the Company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of this section, in respect of such transactions to the Director within the prescribed time.

The formats for reporting the requisite information in respect of cash transactions and suspicious transactions as provided by FIU shall be followed as prescribed from time to time.

For determining integrally connected cash transactions, the Company shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds rupees ten lakh during the month.

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The Company will pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to NHB/other relevant authorities.

It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. The Company shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.
The Company shall make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

Combating financing of terrorism:

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

b. As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the Company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities shall be accessed from the United Nations website at: http://www.un.org/sc/committees/1267/consolist.shtml.

The Company shall before opening any new account, ensure that the name/s of the proposed customer does not appear in the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to FIU-IND. KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the Company as an integral part of recruitment/hiring process of personnel.

The required information shall be furnished by the Company directly to the FIU-IND, through the Principal Officer designated by Company under the Prevention of Money Laundering Act, 2002.

General:

Information collected from the Customer shall be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Company shall therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive and is inconformity with the guidelines issued by RBI in this regard. Company shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment.

Customer Identification Procedure

Features to be verified and documents that will be obtained from customers

Customers/Clients	Documents (Certified Copy)
Individuals: Legal Name and any other names used Correct permanent address for proof of residence of individuals	a. Pan Card (Mandatory) b. Passport c. Voter's Identity Card d. Driving License e. Letter issued by Gazetted Officer with duly attested photograph of the individual f. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company g. Aadhaar card issued by Unique Identification Authority of India containing details of name, address and Aadhaar number. h. Telephone bill (not more than 2 months old) i. Account Statement latest 3 months j. Letter from any recognized public authority. k. Electricity bill l. Property/Municipal Tax Receipt m. Piped Gas Connection Bill/Post Paid Mobile Bill (carrying the present address of the customer, provided that the said bills are not older than 2 months).
Companies: Name of the Company Principal place of business Mailing address of the Company Telephone / Fax Number	Certified copies of the following documents: - a. Certificate of Incorporation (Mandatory); b. Memorandum of Association and Articles of Association (Mandatory); c. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; d. An officially valid document in respect of Mangers, Officers or Employee holding an attorney to transact on its behalf; e. Copy of PAN card (Mandatory); and f. Copy of the Utility Bill (not older than 2 months). g. Letter/Certificate from any recognized public authority
Partnership Firm: - Legal Name - Address - Names of all partners - And their address - Telephone numbers of the firm and partners	Certified copies of the following documents: - a. Registration certificate, if registered; b. Copy of PAN Card (Mandatory); c. Partnership deed (Mandatory); d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf; e. Any officially valid document identifying the partners and the persons holding the power of Attorney and their address; and

	f. Utility Bill (not older than 2 months) in the name of firms / partners
Trusts & Foundation: - Name of trustees, settlers, beneficiaries and signatories - Name and address of the founder, the managers / directors and the beneficiaries - Telephone / fax numbers	Certified copies of the following documents:- a. Registration certificate, if registered; b. PAN Card (Mandatory) c. Trust deed (Mandatory); d. Power of Attorney granted to transact business on its behalf; e. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders / managers / directors and their address; f. Resolution of the managing body of the foundation / association; and g. Utility Bill (not older than 2 months) in the name of trust / trustees
Unincorporated Association or a Body of Individuals	Certified copies of the following documents: - a. Resolution of the managing body of such association or body of individuals; b. Power of attorney granted to him to transact on its behalf; c. Such information as may be required by the reporting entity to collectively establish the legal existence of such an association or body of individuals; d. An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Sole Proprietary Firms/concerns Proof of the name, address and activity of the concern	Certified copy of OVD as applicable to the Individuals (i.e. of proprietor) shall be obtained. In addition to the above, any two of the following documents as a proof of business/activity in the name of the proprietary firm shall also be obtained: a. Registration certificate (in the case of a registered concern) b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act. c. GST and Income tax returns. d. CST/VAT/GST certificate, whenever applicable Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities / GST authorities. e. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. f. 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. g. Utility bills such as electricity, water, and landline telephone bills (not older than 2 months).

	In cases where the Company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as proof of business/activity. In such cases the Company, however would have to 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.

In such cases the Company, however would have to 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.

'Officially Valid Document' is defined to mean the Passport, the Driving License, the Permanent Account Number (PAN) card, the Voter's Identity Card issued by Election Commission of India, Job card issued by NREGA, Aadhaar Card/ letter or any other document as notified by the Central Government.

x-x-x-x-x-x-x