

DEEVEE COMMERCIALS LTD

CIN: L51109WB1983PLC035918

**157C, Lenin Sarani 3rd Floor, Room No. A308, Delux Centre,
Kolkata-700013**

KYC POLICY

Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

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 vide Board Meeting dated February 04, 2017.

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

Objective

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandates making reasonable efforts to determine the true 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 risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

Customer Acceptance Policy

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

- Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk. The illustrative list of such risk categorisation is provided in Annexure 1.
- The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose.
- The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.
- The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting (STR).



Customer Identification Procedure

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

An effective Customer Identification Program ("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 Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

1. **verify the identity of any Person** transacting with the Company to the extent reasonable and practicable;
2. **maintain records of the information** used to verify a customer's identity, including name, address and other identifying information and
3. **consult lists of known or suspected terrorists** or terrorist organizations provided to the Company by any applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.

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

Required KYC Due Diligence for all customers

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

- **Identification:**

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

Each business process shall implement procedures to obtain from each Customer, prior to transacting, the following information as may be relevant, to that business:

1. Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same



as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;

2. For individuals - age/ date of birth; For a person other than individual (such as corporation, partnership or trust) - date of incorporation;
3. Address including the documentary proof thereof;
 - i. For an individual, a residential or business street address;
 - ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;
4. Telephone/Fax number/E-mail ID;
5. Identification number:
 - i. A taxpayer identification number; passport number and country of issuance; letter issued by Unique Identification Authority of India containing AADHAR number; alien identification card 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;
 - ii. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but each business process shall implement 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 of time before disbursement of loan.

Fresh photographs will be obtained from minor customer on becoming major.

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as annexure III to this policy. These are appropriately covered in the credit policies of the respective businesses and communicated to the credit approving authorities.

For proprietary concerns, the company will collect any two documents from the list given in Annexure III and only where the company is satisfied that it is not possible for the customer to furnish two such documents, the company will have the discretion to accept only one of those documents as activity proof. In such a situation, the company will record the appropriate reason for accepting one document as activity proof.

If an existing KYC compliant customer desires to open another account, there is no need for submission of fresh proof of identity and/or proof of address for the purpose.

• **Verification**

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the



true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

i. Verification through documents:

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in Annexure - II to this policy. These are appropriately covered in the credit policies of the respective businesses.

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as annexure II to this policy. These should be appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

ii. Verification through non-documentary methods:

These methods may include, but are not limited to:

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

iii. Additional verification procedures.

If applicable, the business process verification procedures should address situations where:

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The business process associate is not familiar with the documents presented;
3. The Account is opened without obtaining documents;
4. Where the business process is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and
5. If the business process cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

Where a low risk category customer expresses inability to complete the documentation requirements on account of any reason that the Company considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the Company may complete the verification of identity within a period of six months from the date of establishment of the relationship.



• Resolution of Discrepancies

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

• Reporting

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs.10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

- a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to have no economic rationale or bona fide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- e. Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Further, the Principal Officer shall furnish information of the above mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the principal officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

• Records Retention

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

- a. **Transactions for which records need to be maintained:**
 - i. All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
 - ii. All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month



and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.

- iii. 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.
- iv. All suspicious transactions whether or not made in cash.

b. Information to be preserved:

The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

c. Periodicity of retention:

The following records shall be retained for a minimum period of ten years after the related account is closed:

- i. The customer identification information and residence identification information including the documentary evidence thereof
- ii. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least Ten (10) years after such record was created.

The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

• **Customer CIP Notice**

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

• **Existing Customers**

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

• **Reliance on third party due diligence:**

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party, subject to the conditions that



- a. the Company immediately obtains necessary information of such client due diligence carried out by the third party;
- b. the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- c. the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
- d. the third party is not based in a country or jurisdiction assessed as high risk; and
- e. the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

Risk Categorisation

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high risk category customers.

Low risk category customers need not submit fresh proofs of identity and address at the time of periodic updation, in case of no change in status with respect to their identities and addresses and a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they can forward a certified copy of proof of address by mail/post, etc.

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of businesses is provided in Annexure - I. Each business process adopts the risk categorization in their respective credit policies subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc.. Where businesses believe that a particular customer falling under a category mentioned below is in his judgement falling in a different category, he may categorise the customer so, so long as appropriate justification is provided in the customer file.

Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different business divisions should pay special



attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts have to be subjected to intensified monitoring.

The Company shall put in place an appropriate software application/ mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

Risk Management

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures.

As a general rule, the compliance function also provides an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements.

Internal Auditors 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 is put up before the Audit Committee of the Board on quarterly intervals.

Customer Education

The Company may prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC through various training programmes and e-mails.

Appointment of Designated Director / Principal Officer

Mr. Dhiraj Agarwal will be the Designated Director who is responsible for ensuring overall compliance as required under PMIA Act and the Rules. Mr. Pramod Bajoria is designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.



Indicative list for Risk Categorisation

Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk.

Illustrative examples are:

1. Salaried employees whose salary structure is well-defined
2. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
3. Government departments and Government-owned companies
4. Statutory bodies & Regulators

Medium & High Risk Category

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

Illustrative examples of medium risk category customers are:

1. Non Resident customers
2. High Networth Individuals
3. Trust, charities, NGO's and Organization receiving donations
4. Companies having close family shareholding or beneficial ownership
5. Firms with 'sleeping partners'

Illustrative examples of high risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
2. Non face-to-face customers
3. Those with dubious reputation as per public information available
4. Accounts of bullion dealers and jewellers



Customer Identification Requirements

Trust/Nominee or Fiduciary Accounts

In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms

Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.

These requirements may be moderated according to the risk perception e.g. in the case of a public company.

Client accounts opened by professional intermediaries

Where the transaction is with a professional intermediary who in turn is on behalf of a single client, that client must be identified.

Accounts of Politically Exposed Persons (PEPs) resident outside India

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.

The Company offers products primarily to Indian residents only. The Company if extending any finance to non residents should check if he is PEP and check all the information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of credit of the respective businesses supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain the approval of Management Committee to continue the business relationship and subject the account to the KYC due



diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership

(a) where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:

I. "Controlling ownership interest" means ownership of or entitlement to more than twenty five percent of shares or capital or profits of the company;

II. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

(c) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

(f) where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Accounts of non-face-to-face customers

The Company will not do any transactions with non-face-to-face customers.



Customer Identification Procedure

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

KYC Documents for Identification and verification

Identity Proof	<p><u>Individual:</u></p> <ul style="list-style-type: none"> - Valid Passport - Voter identity card issued by Election Commission of India - Valid PAN card - Valid driving license - Job card issued by NREGA duly signed by an officer of the State Government - Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. <p><u>Others:</u></p> <p><u>Company:</u></p> <ul style="list-style-type: none"> - Certification of incorporation - MOA/AOA - Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf - An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf <p><u>Partnership Firms:</u></p> <ul style="list-style-type: none"> - Registration certificate - Partnership deed - An officially valid document in respect of the person holding an attorney to transact on its behalf. <p><u>Trust and Foundations:</u></p> <ul style="list-style-type: none"> - Registration certificate - Trust deed - An officially valid document in respect of the person holding an attorney to transact on its behalf. <p><u>Unincorporated association or body of individuals:</u></p> <ul style="list-style-type: none"> - Resolution of the managing body of such association or body of individuals - Power of attorney granted to him to transact on its behalf - An officially valid document in respect of the person holding an attorney to
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



	<p>transact on its behalf.</p> <ul style="list-style-type: none"> - Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals
Address Proof	<p><u>Individuals:</u></p> <ul style="list-style-type: none"> - Valid passport - Voter identity card issued by Election Commission of India - Valid driving license, - Job card issued by NREGA duly signed by an officer of the State Government - Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. <p><u>Others:</u></p> <p><u>Company:</u></p> <ul style="list-style-type: none"> - Certification of incorporation - MOA/AOA - Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf - An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf <p><u>Partnership Firms:</u></p> <ul style="list-style-type: none"> - Registration certificate - Partnership deed - An officially valid document in respect of the person holding an attorney to transact on its behalf. <p><u>Trust and Foundations:</u> - Registration certificate</p> <ul style="list-style-type: none"> - Trust deed - An officially valid document in respect of the person holding an attorney to transact on its behalf. <p><u>Unincorporated association or body of individuals:</u></p> <ul style="list-style-type: none"> - Resolution of the managing body of such association or body of individuals - Power of attorney granted to him to transact on its behalf - An officially valid document in respect of the person holding an attorney to transact on its behalf. - Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals
Proprietary Concerns	<p><u>For proprietary concerns, the company should call for and verify any two of the following documents:</u></p>



- Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.
- Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. NBFCs/RNBCs may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.
- The 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.
- Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

** Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.*

*** In case of proprietary concern, the documents shall be in the name of the concern.*

Note:

1. All the applicants shall have valid ID proof as prescribed above.
2. 'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the documents mentioned below for the purpose of—

A. Proof of identity –

1. Identity card with applicant's Photograph issued by Central / State Government Departments, Statutory / Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
2. letter issued by a gazetted officer, with a duly attested photograph of the person;

B. Proof of address

The following documents shall be deemed to be officially valid documents for 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any officially valid document for the same:



1. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);
 2. Property or Municipal Tax receipt;
 3. Bank account or Post Office savings bank account statement;
 4. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 5. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
 6. Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.
3. Over and above the KYC identification of the customer as per the process laid in above, in case the customer is residing at an address different from the address mentioned in the proof submitted in accordance with annexure III, the company shall collect any of the documents listed below in addition to one address proof as listed in annexure III for communication/contact address:-

- a. Latest Telephone bill – landline and postpaid mobile bills (Not more than six months old)
- b. Latest Utility bills (Not more than six months old)
- c. Bank account statement (Not more than six months old)
- d. Registered Lease deed along with utility bill in the name of the landlord



Illustrative list of activities which would be construed as suspicious transactions

- Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
 - A 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.
 - An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- Certain Employees of the Company arousing suspicion:
 - An employee whose lavish lifestyle cannot be supported by his or her salary.
 - Negligence of employees/willful blindness is reported repeatedly.
- Some examples of suspicious activities/transactions to be monitored by the operating staff:
 - Multiple accounts under the same name
 - Refuses 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