

---

**Know Your Customer (KYC) & Prevention of Money Laundering (PMLA) Policy Policy version: NBFC/KYC-PMLA/Mar-2014**

## Contents

<b>A. INTRODUCTION</b> .....	<b>3</b>
<b>B. OBJECTIVES</b> .....	<b>3</b>
<b>C. DEFINITION OF CUSTOMER</b> .....	<b>4</b>
<b>Know Your Customer Standards</b> .....	<b>4</b>
I. Customer Acceptance Policy (CAP).....	4
II. Customer Identification Procedure (CIP).....	6
III. Monitoring of Transactions .....	7
IV. Maintenance of records of transactions .....	9
V. Preservation of records .....	9
VI. Reporting to Financial Intelligence Unit-India .....	10
VII. Risk Management.....	10
VIII. Customer Education .....	11
IX. Introduction of New Technologies - Credit cards.....	11
X. Combating financing of terrorism.....	11
XI. Appointment of Compliance/Principal Officer .....	12
<b>ANNEXURE I: CUSTOMER IDENTIFICATION PROCEDURE</b> .....	<b>13</b>
<b>ANNEXURE II: CUSTOMER IDENTIFICATION REQUIREMENTS – Indicative Guidelines</b> .....	<b>15</b>
<b>Annexure III: AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES</b> .....	<b>17</b>

## **A. INTRODUCTION**

Micro Capitals Private Limited ('The company') commits itself to the highest standards of transparency, compliance and fair practices while meeting the business loan needs of various kind of borrowers in a timely and effective manner. The company's business, be conducted in accordance with the prevailing statutory and regulatory requirements with due focus on efficiency, customer-orientation and corporate governance principles

The Reserve Bank of India (RBI) had advised all NBFCs; vide its circular dated January 2004, to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. Following the recommendations made by the Financial Action Task Force (FATF) in 2005, these guidelines were revisited to include instructions on Anti-Money Laundering (AML) Standards and Combating Financing of Terrorism (CFT)

The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this code to conform to the standards so prescribed. This policy is applicable across all branches / business segments of the company, and its financial subsidiaries as well as all the persons authorised by NBFCs including agents /intermediaries, or brokers collecting public deposits on behalf of the NBFC (presently we do not accept public deposits and this will be applicable when we are authorised to do so). The Policy is to be read in conjunction with related operational guidelines issued from time to time and necessarily read with reference to the changes/modifications as advised by RBI from time to time.

The Company is committed to the highest standards of transparency and fairness in dealing with all stakeholders and in ensuring adherence to all applicable laws and regulations. Any information collected from the customer for any purpose (account opening, sanction, etc) would be kept confidential and any details thereof would not be divulged for cross selling or any other purposes. The Company will ensure that any information sought from the customer is relevant to the perceived risk, 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 his/her consent and after opening the account.

The Company's Board of Directors/ Risk Management Committee will be responsible for:

- ü Communicating the KYC norms to its customers
- ü Implementing the detailed KYC norms
- ü Ensure that necessary initiatives are taken to prevent Money laundering activities

This policy shall be known as the 'Know Your Customer (KYC) & Prevention of Money Laundering Act (PMLA) Policy'

## **B. OBJECTIVES**

The objective of the KYC guidelines is

- i. To put in place systems and procedures to help control financial frauds, identify money laundering and suspicious activities

- ii. To safeguard the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities;
- iii. To put in place systems and procedures for customer identification and verifying his / her identity; as well as understand the customer's financial dealings, which in turn help us manage risks prudently
- iv. To monitor transactions of a suspicious nature.

#### **C. DEFINITION OF CUSTOMER**

For the purpose of this KYC & PMLA policy, a Customer is:

- i. a person or entity that maintains an account and/ or has a business relationship with the Company in any capacity, whether as an individual or otherwise as explained herein;
- ii. one on whose behalf, the account is maintained i.e. the beneficial owner(s)
- iii. beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants and Solicitors etc. as permitted under law;
- iv. any other person or entity connected with a financial transaction, which can pose significant reputational or other risks to the Company (eg issue of high value demand draft as a single transaction, etc)

Thus, the definition includes but is not limited to individuals, companies, partnership firms, banks, mutual funds, Limited Liability Partnerships, unincorporated entities, trusts and/or overseas corporate bodies.

### **Know Your Customer Standards**

The Company's KYC policies incorporate the following four key elements:

- i. Customer Acceptance Policy
- ii. Customer Identification Procedures;
- iii. Monitoring of Transactions; and
- iv. Risk management

#### **I. Customer Acceptance Policy (CAP)**

The CAP guidelines for the Company are given below:

- o No account is opened in anonymous or fictitious/ benami name(s).
- o The Company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category
- o Parameters of risk perception shall be 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; customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorized even higher;
- o Accept customers after verifying their identity as laid down in customer identification procedures
- o While carrying out due diligence the company shall ensure that the procedure adopted shall not result in denial of services to the genuine customers
- o For the purpose of risk categorisation of customer, company shall obtain the relevant information from the customer at the time of account opening

- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;
- The company shall not to open an account or close an existing 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 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;
- 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 practice of banking as there shall be occasions when an account is operated by a mandate holder or where an account shall be opened by an intermediary in the fiduciary capacity; and
- 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 etc.
- The company shall prepare a profile for each new customer based on risk categorisation. 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 etc. The nature and extent of due diligence shall 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. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes
- 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 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 and his client profile 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
- Examples of customers requiring higher due diligence may 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.
- Adoption of customer acceptance policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged
- As advised by RBI under Circular No. DNBS(PD)CC.No.193/03.10.42/2010-11, the Company shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client

## II. Customer Identification Procedure (CIP)

The policy, as approved by the Board of the Company clearly spells out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. 'Being satisfied' means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to 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 shall 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

- Verify the legal status of the legal person / entity through proper and relevant documents
- 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,
- Understand the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person; The Company shall take into account Customer identification requirements in respect of a few typical cases, especially; legal persons requiring an extra element of caution are given in Annexure-II as per Circular No.: DNDS (PD) CC NO. 48/10.42/2004-05 dated 21-02-2005 for guidance of NBFCs.
- The Company shall frame 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.

- The Company shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the Annexure I.
- 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.
- The documents 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 is to 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.
  - 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 Head 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 from time to time.

### III. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. 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 shall depend on the risk sensitivity attached with the client.

- The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.
- The Company normally does not and would not have large cash transactions. However, if and when cash transactions of Rs.10 lakhs and above are undertaken for a particular category of clients and pay particular attention to the transactions which exceed these limits and also keep a record of the same
- Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. The company does not accept any deposits.
- Further, there are no operative accounts where in the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary.
- All the company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the company are purely shall be restricted to the EMI payable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions what so ever nature other than repayment of loan with interest is carried out by the customer with the company.
- As per RBI Circular No. RBI/2010-11/419 DNBS (PD) CC No 212/03.10.42/2010-11 NBFCs were further advised that in view of the risks involved in cash intensive businesses, accounts of bullion dealers

(including sub-dealers) and jewelers should also be categorized by NBFCs as 'high risk' requiring enhanced due diligence. The Company shall implement the same and classify such bullion dealers and jewelers under "high risk" category and any transactions in their loan accounts would be monitored on daily basis.

- The permanent correct address shall mean the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative: wife, son, daughter and parents etc. who live with their husband, father/mother and son, the company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The company shall use any supplementary evidence such as a letter received through post for further verification of the address.
- While issuing operational instructions to the branches on the subject, the company shall keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.
- Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts shall be subjected to intensified monitoring. The company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. 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.
- The company shall ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority.
- The company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation 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 five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories
- The Company shall ensure that its branches continue to maintain proper record of all cash transactions. 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.
- Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the "offence of money laundering" as under: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".
- The Company shall adopt the guidelines issued by RBI for Prevention of Money Laundering vide Circular No. DNBS (PD) CC No. 48/10.42/2004-05 dated 21-02-2005. All transactions of cash and suspicious as required under PML Act 2002 shall be reported to FIU from time to time. The Principal Officer specified by the company shall ensure that such reporting system is in place and shall monitor receipt of the reports.
- The name of the Principal Officer shall be specified by the CEO of the company from time to time. All transactions of suspicious nature and / or any other type of transaction notified under section '12 of the



PML Act, 2002, shall be reported to the appropriate law enforcement authority by the Principal Officer

IV. Maintenance of records of transactions

The Company shall introduce a system of maintaining proper record of transactions prescribed under rule 3, as mentioned below:

- all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- 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;
- 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 in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

V. Preservation of records

The Company shall maintain the following information in respect of transactions referred to in rule 3:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.
  
- The company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, the company shall maintain for at least ten years from the date of cessation of transaction between the company and the client, all necessary records of transactions, both domestic or international, which shall permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.
- The company shall 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, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended.
- The identification records and transaction data shall be made available to the competent authorities upon request

## VI. Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, the company shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

- The Company shall adopt the format prescribed; follow timelines, guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. The company shall initiate urgent steps to ensure electronic filing of cash transaction report (CTR). The Company shall not put any restrictions on operations in the accounts where an STR has been made. However, it shall be ensured that there is no tipping off to the customer at any level.
- For determining integrally connected cash transactions, NBFCs 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 shall 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 Reserve Bank/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 .
- In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the company shall consider the indicative list of suspicious activities contained in Annex-III

## VII. Risk Management

The Board of Directors of the Company shall ensure that an effective KYC program 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.
- Non-Deposit taking NBFCs with assets of Rs 25 cr and above and all Deposit taking NBFCs have to put in place a unique customer identification code (UCIC). The UCIC will help NBFCs to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable NBFCs to have a better approach to risk profiling of customers. It would also smoothen NBFC's operations for the

- customers
- The Company shall, in consultation with their 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 independent evaluation of the Company's own policies and procedures including legal and regulatory requirements. The Company shall ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent / 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 shall be put up before the Audit Committee of the Board on quarterly intervals.
  - The Company shall put in place an ongoing employee training program 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

#### VIII. Customer Education

Implementation of KYC procedures requires the Company to demand certain information from customers which shall be of personal nature or which have hitherto never been called for. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company shall prepare specific literature/pamphlets etc. so as to educate the customer of the objectives of the KYC program. The front desk staffs shall be specially trained to handle such situations while dealing with customers.

#### IX. Introduction of New Technologies - Credit cards

The Company shall pay special attention to any money laundering threats that shall arise from new or developing technologies including internet transactions that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many Companies are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds.

Further, marketing of these cards is generally done through the services of agents. The Company shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers, if any, in future; agents shall also be subjected to KYC measures.

#### X. Combating financing of terrorism

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.

- 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 in 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 RBI and FIU-IND.
- KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the company as an integral part of recruitment/hiring process of personnel.
- The company shall take into account risks arising from the deficiencies in AML/CFT regime of countries of Iran, Angola, Democratic People's Republic of Korea (DPRK), Ecuador, Ethiopia, Pakistan, Turkmenistan and Sao Tome and Principe and list of countries circulated by RBI from time to time, whenever applicable
- In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the company shall consider the indicative list of suspicious activities contained in Annex-III

Applicability to branches and subsidiaries outside India (Presently we do not have any branches outside India, shall be applicable when ever branches are opened outside India)

The extant instructions that KYC/AML guidelines issued by RBI shall also apply to their branches and majority owned subsidiaries located outside India, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. It is further clarified that in case there is a variance in KYC/AML standards prescribed by the RBI and the host country regulators, branches/overseas subsidiaries of the company shall adopt the more stringent regulation of the two.

#### XI. Appointment of Compliance/Principal Officer

The Company has a senior management officer to be designated as Compliance/Principal Officer. Compliance/Principal Officer shall be located at the head/corporate office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He shall maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The Manager appointed under Companies Act shall be the Compliance/ Principal Officer of the Company for this purpose.

This document is the property of the Company. It contains information that is internal to the company and is of competitive value and sensitive in nature. All employees must treat its contents as confidential and keep it secure.

**ANNEXURE I**  
**Customer Identification Procedure**

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

Features	Documents
<p>Accounts of individuals</p> <ul style="list-style-type: none"> <li>- Legal name and any other names used</li> <li>- Correct permanent address</li> </ul>	<p>(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) ( any one document which provides customer information to the satisfaction of the bank will suffice )</p>
<p>Accounts of companies</p> <ul style="list-style-type: none"> <li>- Name of the company</li> <li>- Principal place of business</li> <li>- Mailing address of the company</li> <li>- Telephone/Fax Number</li> </ul>	<p>(i) Certificate of incorporation and Memorandum &amp; Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill</p>
<p>Accounts of partnership firms</p> <ul style="list-style-type: none"> <li>- Legal name</li> <li>- Address</li> <li>- Names of all partners and their addresses</li> <li>- Telephone numbers of the firm and partners</li> </ul>	<p>(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses</p>

	(v) Telephone bill in the name of firm/partners
<p>Accounts of trusts &amp; foundations</p> <ul style="list-style-type: none"> <li>- Names of trustees, settlers, beneficiaries and signatories</li> <li>- Names and addresses of the founder, the managers/directors and the beneficiaries</li> <li>- Telephone/fax numbers</li> </ul>	<p>(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses</p> <p>(iv) Resolution of the managing body of the foundation/association</p> <p>(v) Telephone bill</p>

**ANNEXURE II:**  
**CUSTOMER IDENTIFICATION REQUIREMENTS – Indicative Guidelines**

**a) Trust/Nominee or Fiduciary Accounts**

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, 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. While opening an account for a trust, the Company shall take 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. Beneficiaries shall be identified when they are defined. Where the client is a trust, the Company, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership. In the case of a 'foundation', steps shall be taken to verify the founder managers/ directors and the beneficiaries, if defined.

**b) Accounts of companies and firms**

The Company needs to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks/ the Company. The Company shall examine the control structure of the entity, determine the source of funds 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 listed public company it shall not be necessary to identify all the shareholders.

**c) Client accounts opened by professional intermediaries**

When the Company has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the Company shall still look through to the beneficial owners. Where the Company relies on the 'customer due diligence' (CDD) done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It shall be understood that the ultimate responsibility for knowing the customer lies with the Company.

**d) 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 shall 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. The Company shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP shall be taken at a senior level which shall be clearly spelt out in Customer Acceptance policy. The Company shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Customer Due Diligence (CDD) measures shall be made applicable to Politically Exposed Person (PEP) and their family members or close relatives. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the company shall obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

**e) Accounts of non-face-to-face customers**

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In such cases, the Company may also require the first payment to be effected through the customer's account with a bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.



**ANNEXURE III**  
**AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES**

**a) Transactions Involving Large Amounts of Cash**

Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

**b) Transactions that do not make Economic Sense**

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnishes a plausible reason for immediate withdrawal

**c) Activities not consistent with the Customer's Business**

Accounts with large volume of credits whereas the nature of business does not justify such credits

**d) Attempts to avoid Reporting/Record-keeping Requirements**

- 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 a NBFC employee not to file any reports 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.

**e) Unusual Activities**

Funds coming from the countries/centers which are known for money laundering

**f) Customer who provides Insufficient or Suspicious Information**

- A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
- A customer/company who is reluctant to reveal details about its activities or to provide financial statements
- A customer who has no record of past or present employment but makes frequent large transactions

**g) Certain NBFC Employees arousing Suspicion**

- An employee whose lavish lifestyle cannot be supported by his or her salary.
- Negligence of employees/willful blindness is reported repeatedly.