MEGHA FINLOAN PRIVATE LIMITED

POLICY ON KNOW YOUR CUSTOMER

&

ANTI-MONEY LAUNDERING("AML") MEASURES

I. PURPOSE

The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) Policy for all Non-Banking financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) policies as these being used as the International Benchmark for framing the stated policies, by the regulatory authorities. In view of the same, Megha Finloan Private Limited (the "Company") has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures are formulated in line with the prescribed RBI guidelines and duly approved by the board.

II. OBJECTIVES, SCOPE AND APPLICATION OF THE POLICY

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risk prudently. Thus, the KYC Policy has been framed by the Company for the following purposes:

1. To prevent criminal elements from using Company for money laundering activities;

2. To enable Company to know and understand its Customers and their financial dealings better which, in turn, would help the Company to manage risk prudently;

3. To put in appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;

4. To comply with applicable laws and regulatory guidelines;

5. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. This KYC Policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time. This Policy includes the following key elements:

a. Customer Acceptance Policy (CAP);
b. Risk Management
c. Customer Identification Procedures (CIP);
d. Money Laundering and Terrorist Financing Risk Assessment;
e. Record Management;
f. Monitoring of Transactions;
g. Training Programme;
h. Internal Control System.

III. DEFINITIONS

i. **Customer:** For the purpose of Company's KYC policy a "Customer" means a Person as defined under Know Your Customer Guidelines issued by RBI (and any amendment from time to time by RBI) which are at present as under:

a. A person or entity that maintains an account and/or has a business relationship with the Company;

b. A Person who has a Registered Account with Company and has a financial transaction or activity with the Company;

c. A Person on whose behalf the Registered Account is maintained (i.e. the beneficial owner);

d. Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law;

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

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:

a. an Individual;
b. a Hindu Undivided Family;
c. a Company;
d. a Firm;
e. an Association of Persons or a Body of Individuals, whether incorporate or not;
f. every artificial juridical person, not falling within any one of the above person (a to e);
g. any agency, office or branch owned or controlled by any one of the above persons (a to f).

ii. "**Aadhaar Number"** shall have the meaning assigned to it in clause(a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

iii. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto;

iv. "Authentication", in the context of Aadhaar authentication, means the process as defined under clause (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

v. "Certified Copy"- Obtaining a Certified Copy shall mean comparing the copy of the proof of possession of Aadhaar Number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the RE as per the provisions contained in the Act;

vi. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer;

vii. "Designated Director" means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. The Managing Director or a whole-time Director, duly authorized by the Board of Directors.

Explanation- For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

viii. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Company as per the provisions contained in the Act;

ix. "Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000;

x. "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016;

xi. "Know Your Client Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry;

xii. "Officially Valid Document (OVD)" means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by MNREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a. Where the Customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India;

b. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- Property or municipal tax receipt;
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

c. The Customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above;

d. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation- For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiii. "Offline Verification" shall have the same meaning as assigned to it in clause(pa) of section(2) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

xiv. "Person has the same meaning assigned in the Act and includes:

a. An individual;
b. A Hindu Undivided Familiy;
c. A Company;
d. A Firm;
e. An Association of persons or a body of individuals, whether incorporated or not;

f. Every artificial juridical person, not falling within any of the above persons (a) to (e), and
g. Any agency, office or branch owned or controlled by any of the above persons (a) to (f).

xv. "Principal Officer" means an officer nominated by the company, responsible for furnishing information as per rule 8 of the Rules;

xvi. "Suspicious Transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. Appears to be made in circumstances of unusual or unjustified complexity; or
c. Appears to not have 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

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

xvii. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. Opening of an account;
b. Deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
c. The use of a safety deposit box or any other form of safe deposit;
d. Entering into any fiduciary relationship;
e. Any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. Establishing or creating a legal person or legal arrangement.

IV. KEY ELEMENTS

1. Customer Acceptance Policy ("CAP"):

(i) The Company's CAP lays down the criteria for acceptance of Customers. The guidelines in respect of Customer relationship in the Company broadly includes the following:

a. No account/file is to be opened/generated in anonymous or fictitious/benami name(s)/entity(ies);

b. Accept Customer only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before creating a new file for lending loan are to be ensured so 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;

c. Classify Customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of Customers. Also, a profile of each Customer will be prepared based on risk categorization. Customer requiring very high level of monitoring, e.g. Politically Exposed Persons as explained in Annexure I may, if considered necessary, be kept in the High Risk Category.

d. Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA) and RBI/Company's guidelines/instructions.

e. Not to open an account or close an existing loan account (except as provided in this Policy), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed, as per the risk categorization, due to non-cooperation of the Customer or non-reliability of the data/information furnished to Company. Suitable built-in safeguards shall be provided to avoid any harassment to Customers.

f. Implementation of CAP should not become too restrictive and result in denial of the Company services to general public.

g. The decision to open a loan account for Politically Exposed Person (PEP) should be taken at senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the Customer explaining the reasons for such a decision.

h. 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 and shall be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

(ii) The Company shall prepare a profile for each new Customer during the credit appraisal based on risk categorization as mentioned in this Policy in Annexure I. The Customer profile shall contain the information relating to the Customer's identity, social and financial status and nature of employment or business activity. The nature and extent of due diligence will depend on the risk perceived by the Company. At the time of credit appraisal of the Customer the details are recorded along with his profile based on the documents provided by the Customer and verified by Company either by itself or through third party sources. The documents collected will be as per the product norms as may be in practice. However, while preparing Customer profile, the Company shall seek only such information from the Customer which is relevant to the risk category and is not intrusive. Any other information

from the Customer should be sought separately with his/her consent and after opening the Registered Loan Account. The Customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes.

(iii) As per KYC Policy, for acceptance and identification, Company's Customers shall be categorized based on perceived risk broadly into three categories- A, B & C. Category A includes High Risk Customers, Category B contain Medium Risk Customers while Category C Customers include Low Risk Customers. None of the Customers will be exempted from Company's KYC procedure, irrespective of the status and relationship with Company or its promoters. The above requirement may be moderated according to the risk perception as explained in Annexure I.

(iv) (A) High Risk – (Category A):

High Risk Customers typically includes:

a. Non-Resident Customers;
b. High Net Worth Individuals without an occupation track record of more than 3 years;
c. Trust, Charitable Organizations, Non-Government Organization (NGO), organizations receiving donations;
d. Companies having close family shareholding or beneficial ownership;
e. Firms with sleeping partners;
f. Politically exposed persons (PEPs) of Indian/foreign origin;
g. Non Face-to-Face Customers;
h. Person with dubious reputation as per public information available;

(B) Medium Risk – (Category B):

Medium Risk Customers will include:

a. Salaried applicant with variable income/unstructured income receiving Salary in cheque;
b. Salaried applicant working with Private Limited Companies, Proprietary, Partnership Firms;
c. Self-employed professionals other than HNIs;
d. Self-employed customers with sound business and profitable track record for a reasonable period;
e. High Net worth individuals with occupation track record of more than 3 years.

(C) Low Risk – (Category C):

Low Risk Individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories. Customer carrying low risk may include the following:

a. Salaried employees with well-defined salary structures for over 5 years;
b. People working with government owned companies, regulators and statutory bodies, MNC's, rated companies public sector units, public limited companies, etc. in the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company will obtain senior management approval in such cases to continue the

business relationship with such person, and also undertake enhanced monitoring as indicated and specified in Annexure I;

c. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
d. People working with Public Sector Units;
e. People working with reputed Public Limited Companies and Multinational Companies.

2. Risk Management:

The Management of the Company under the supervision of the Board of Directors and the Loan and Risk Committee shall 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 will be explicitly allocated within the Company for ensuring that the policies and procedures as applicable to Company are implemented effectively. The Company shall 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. For risk categories, refer point 1 (Customer Acceptance Policy).

3. Customer Identification Procedures ("CIP"):

(i) Customer Identification means identifying the Customer and verifying his/her identity by using reliable, independent source documents, data or information. Company shall obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship as specified in Annexure I and Annexure IV. The requirement as mentioned herein may be moderated according to the risk perception for e.g. in the case of a public limited company it may not be necessary to identify all the shareholders.

(ii) 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, 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;

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.

(iii) Understand the ownership and control structure of the Customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements keeping in view the provisions applicable of Prevention of Money Laundering & its Rules and as per guidance note issued in this respect are indicated in Annexure I. An indicative list of the nature and type of documents/information that may be relied upon for Customer Identification is given in Annexure II. The Company will frame internal guidelines based on its experience of dealing with such persons/entities, normal prudence and the legal requirements.

(iv) The Company will formulate and implement a Customer Identification Programme to determine the true identity of its Customers keeping the above in view. The Policy shall also cover the Identification Procedure to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when there is a doubt about the

authenticity/veracity or the adequacy of the previously obtained Customer Identification data.

Important: The Company shall periodically update Customer Identification Data after the transaction is entered. The periodicity of updating of Customer Identification data shall be once in five years in case of Low Risk Category Customers and once in two years in case of High and Medium Risk Categories.

4. Money Laundering and Terrorist Financing Risk Assessment:

a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time;

b. The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually;

c. The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

The company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, company shall monitor the implementation of the controls and enhance them if necessary.

Accordingly, the below mentioned priority areas for addressing the threats and vulnerabilities of Money Laundering/Terrorists Financing risk in NBFC Sector shall be carried out while carrying out internal ML/TF Risk assessment:-

- Effectiveness of Suspicious Activity Monitoring and Reporting
- Availability and Access to Beneficial Ownership Information
- Effectiveness of Compliance Function (Organization)
- Integrity of Business/Institution Staff

5. Record Management:

i. **Maintenance of records of transactions:** The Company shall maintain proper record of the transactions as required under Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:

a. All cash transactions of the value of more than Rupees Ten Lacs (Rs. 10,00,000/-) or its equivalent in foreign currency, though by policy the Company neither accept cash deposits nor in foreign currency.

b. All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lacs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month.

c. All transactions involving receipts by non-profit organizations of Rupees Ten Lacs 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 has taken place; any such transactions.

e. All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure IV.

ii. **Records to contain the specified information: The Records referred to above in Rule 3 of PML Rules to contain the following information:**

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;

d. the parties to the transaction.

iii. Maintenance and preservation of records Section 12 of PML Act requires the Company to 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 is required to be maintained for a period of Ten (10) years from the date of transactions between the Customers and Company.

b. records of the identity of all Customers of Company are required to be maintained for a period of Ten (10) years from the date of cessation of transactions between the Customers and Company.

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

iv. Appointment of Principal Officer:

Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. Principal Officer shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT.

v. Reporting to Financial Intelligence Unit-India:

The Principal Officer shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIU-India) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director,
Financial Intelligence Unit India,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi-110021

The employees of the Company shall maintain strict confidentiality of the fact of furnishing/reporting details of suspicious transactions.

6. 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. Company shall make endeavours 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. Company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of Company. Higher risk accounts shall be subjected to intense monitoring. Company shall set key indicators for such accounts basis the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. Company shall carry out the periodic review of risk categorization of transactions/customer's accounts 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 account opening applications with various watch lists available in public domain, including RBI watch list.

7. Training Programme:

Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/AML/CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC Policies and implement them consistently.

8. Internal Control System:

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC Policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management of the Company under the supervision of the Committee shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will 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 Committee along with their normal reporting frequency. Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/hiring process of personnel so as to ensure that person of criminal nature/background do not get an access, to misuse the financial channel.

GENERAL:

I. Customer Education:

Company shall educate Customers on the objectives of the KYC programme so that Customer understands and appreciates the motive and purpose of collecting such information. The Company shall prepare specific literature/pamphlets, terms and conditions etc. so as to educate the Customer about the objectives of the KYC programme. The front staff shall be specially trained to handle such situations while dealing with Customers.

II. Introduction of New Technologies:

Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering. 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.

III. 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, Company shall terminate Financing/Business Relationship after issuing notice to the Customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Chairman & Managing Director or Key Managerial person(s) authorized for the purpose.

IV. KYC for the Existing Accounts:

While the KYC Policy will apply to all new Customers, the same would be applied to the existing Customers on the basis of materiality and risk. However, transactions with existing Customers would be continuously monitored for any unusual pattern in the operation of the accounts.

V. Updation in the KYC Policy of Company:

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

ANNEXURE-I

CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

I. Loan 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. Branch/office 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. Branch/office 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 provide financial services to an account for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

II. Trust/Nominee or Fiduciary Accounts:

Branch/offices shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the Persons on whose behalf they are reacting, as also obtain details of the nature of the trust or other arrangements in place. The Company shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any Person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a foundation, branches shall take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer Identification Procedures.

III. Accounts of Companies and Firms:

Branch/office need to be vigilant against business entities being used by individuals as a front for maintain accounts with NBFCs. Branch/office may 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.

ANNEXURE-II

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers

Customers/Clients	**Documents** **(Certified copy of anyone of the following officially valid document)**
Individuals (Applicant/Co-Applicant) - Proof of Identity and Address	a) *Passport; b) PAN Card; c) Voter's Identity Card; d) Driving License; e) Identity Card (subject to the Company's satisfaction); f) Aadhaar Card; g) Letter from a recognized public authority or public servant verifying the identity and residence of the Customer to the satisfaction of the Company. a) Telephone bill; b) Bank Account Statement; c) Letter from any recognized public authority; d) Electricity bill; e) Letter from employer (subject to the Company's satisfaction). Any one document which provides Customer information to the satisfaction of the Company will suffice. One recent photograph except in case of transactions referred to in Rule 9 (1) (b) of the PML Rules.
Accounts of Companies - Name of the Company. - Principal place of business. - Mailing address of the Company. - Telephone/Fax Number.	a) Certificate of incorporation and Memorandum & Articles of Association; b) Resolution of the board of directors to open an account and identification

	of those who have authority to operate the account; c) Power of attorney granted to its managers, officers or employees to transact business on its behalf; d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf; e) Copy of PAN allotment letter; f) Copy of telephone bill.
Accounts of Trusts and foundations - Names of trustees, settlers, beneficiaries and signatories.	a) Certificate of registration, if registered; b) Trust Deed; c) Power of attorney granted to transact business on its behalf; d) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding power of attorney, founders/ managers/ directors and their addresses; e) Resolution of the managing body of the foundation/association; f) Telephone bill.

∗ Compulsory in case of non resident individuals.

If any of the above documents are in any language other than English, it shall be translated into English along with a certificate from translator/notary public.

∗ 'Officially valid document' is defined to mean the passport, the driving license, the permanent account number card, the Voter's Identity Card issued by the Election Commission of India or any other document as may be required by the Company.

ANNEXURE III
ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTION PERTAINING TO FINANCIAL SERVCIES

Broad categories of reason for suspicion and examples of suspicious transactions for Non-Banking Financial Companies are indicated as under:

1. **Identity of Client:**
   a) False identification documents
   b) Identification documents which could not be verified within reasonable time
   c) Accounts opened with names very close to other established business entities.

2. **Background of Client:**
   Suspicious background or links with known criminals.

3. **Multiple Accounts:**
   Large number of accounts having a common account holder, introducer or authorized.

4. **Signatory with no rationale:**
   Unexplained transfers between multiple accounts with no rationale.

5. **Activity in accounts:**
   a) Unusual activity compared with past transactions- Sudden activity in dormant accounts;
   b) Activity inconsistent with what would be expected from declared business.

6. **Nature of transactions:**
   a) Unusual or unjustified complexity;
   b) No economic rationale or bonafide purpose;
   c) Frequent purchases of drafts or other negotiable instruments with cash;
   d) Nature of transactions inconsistent with what would be expected from declared business.

7. **Value of Transactions:**
   a) Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
   b) Value inconsistent with the Client's apparent financial standing.

8. **Illustrative list of Suspicious Transactions:**
   a) Reluctant to part with information, data and documents;
   b) Submission of false documents, purpose of loan and detail of accounts;
   c) Reluctance to furnish details of source of funds of initial contribution;
   d) Reluctance to meet in person, representing through power of attorney;
   e) Approaching a distant branch away from own address;
   f) Maintaining multiple accounts without explanation;
   g) Payment of initial contribution through unrelated third party account;
   h) Suggesting dubious means for sanction of loan;
   i) Where transactions do not make economic sense;
   j) Where doubt about beneficial ownership;
   k) Encashment of loan through a fictitious bank account;

l) Sale consideration quoted higher or lower than prevailing area prices;
m) Request for payment in favour of third party with no relation to transaction;
n) Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent;
o) Multiple funding involving NGO, Charitable organization, small and medium establishments, self-help groups, micro finance groups, etc.;
p) Frequent request for change of address;
q) Over-payment of instalments with a request to refund the overpaid amount.