KYC & PMLA POLICY

[Based on Reserve Bank of India's (RBI) Know Your Customer (KYC) Directions, 2016 and Prevention of Money Laundering Act (PMLA) 2002, Rules framed there under]

4Fin Finance Private Limited

Contents

1. BACKGROUND

Reserve Bank of India ["RBI"], has issued the Know Your Customer (Reserve Bank) Directions, 2016 [the "KYC Directions"] bearing reference DBR. AML. BC. No. 81/14.01.001/2015-16 dated 25th February, 2016, as amended upto 10th May, 2021. The said directions are applicable to the Company, being a Non- Banking Financial Company having customer interface. The guidelines mainly address the risks associated to KYC Procedures, Anti Money Laundering ["AML"] Standards, regulations under the Prevention of Money Laundering Act ["PMLA"], and the recommendations of the Financial Action Task Force ["FATF"] on AML Standards.

In view of the same, 4Fin Finance Private Limited [the "Company"], has framed this KYC and PMLA Policy [this "Policy"], based on the policy framework prescribed by RBI under the KYC Directions and PMLA, along with suitable stricter modifications based on the risk matrix of the Company's operations.

2. OBJECTIVES AND SCOPE

This policy has been framed for attaining the following objectives:

a) To prevent criminal elements from using Company for money laundering activities.
b) To enable the Company to know and understand its customers and financial dealings in a better manner, which in turn, shall help manage the risks prudently.
c) To establish appropriate, effective and efficient controls for detection and reporting of suspicious activities in accordance with the applicable laws / laid down procedures.
d) To comply with the applicable regulations and operate within the regulatory framework prescribed by the regulator.
e) To ensure importance of KYC / AML / Combating the Financing of Terrorism ["CFT"] is established with the concerned employees / persons dealing with customers on behalf of the Company.
f) To ensure adequate training to the employees / persons dealing with customers on behalf of the Company in the KYC / AML / CFT procedures.

This policy shall be applicable organization-wide to all employees / persons dealing with customers on behalf of the Company.

This policy is to be read in conjunction with the operational guidelines issued from time to time. The content of this policy shall always be read in tandem / auto-corrected with the changes / modifications as may be advised by RBI and / or by PMLA and amendments of the Directions, from time to time.

Note: Terms used under this policy and not defined hereunder shall have the same meaning as assigned to them under the Directions. The Directions will have a superseding effect on the policy.

3. DESIGNATION OF RESPONSIBILITY AND MANAGEMENT

The Board of Directors of the Company shall be responsible for the purposes of compliance with the KYC/ AML / CFT procedures of the Company.

The Principal Officer of the Company, so appointed, shall be responsible for effective and complete implementation of the procedures prescribed under this policy.

The Company shall devise the internal audit function in a manner, which shall extensively include verification of KYC / AML / CFT procedures undertaken by the Company, and its compliance with this policy and regulatory requirements.

4. DESIGNETED DIRECTOR

The Company has appointed Whole Time Director / Managing Director of the Company, as the Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and the Rules, as nominated by the Board of Directors. The Designated Director of the Company shall not be the same as the Principal Officer of the Company.

5. PRINCIPAL OFFICER

The Company shall designate a senior employee as a Principal Officer (PO), who shall be located at Head/Corporate Office and not be the same as the Designated Director, for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. PO shall maintain close liaison with enforcement agencies, NBFCs, Credit Information Companies, FIU-Ind, and any other institutions involved in the fight against money laundering and CFT.

6. CHANGES IN OFFICERS

The Company shall intimate the Regional Office of RBI, along with the office of Financial Intelligence Unit – India ["FIU-Ind"], of any change in the Principal Officer and / or Designated Director of the Company and/ or their details within one month of the date of such change.

7. CUSTOMER

For the purposes of this policy, "Customer" shall mean a person, engaged in a financial transaction / activity with the Company and includes a person on whose behalf the person who is engaged in the transaction / activity, is acting.

"Person" for the purposes of this policy shall include:

a. An Individual
b. A Hindu Undivided Family
c. A Company
d. A Firm
e. An Association of Persons / Body of Individuals, whether incorporated or not
f. Every artificial juridical person, not falling within any one of the above persons
g. Any agency / Office / Branch owned / controlled by any of the persons above

8. BENIFICAL OWNER

a. Where the customer is a **COMPANY**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have controlling ownership interest(s) or who exercise control through other means.

"Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

"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 customer 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/have ownership of/entitlement to more than 15 percent of capital or profits of the partnership.

c. Where the customer 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/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or(c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, 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.

9. OFFICIALLY VALID DOCUMENTS

Officially Valid Documents ["OVD"] for the purposes of this policy shall include:

a. Passport
b. Driving License
c. Proof of possession of Aadhaar number
d. Voter's Identity Card issued by Election Commission of India
e. Job Card issued by NREGA, duly signed by an officer of the State Government
f. Letter issued by 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: -

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by State 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.

Note:- For the purpose of this, 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.

10. CUSTOMER ACCEPTANCE POLICY

The Company's Customer Acceptance Policy ["CAP"] lays down the basic criteria for acceptance of customers, with the framework constituted of the following:

a. The Company is strictly prohibited to engage into any financial transaction / account based relationship with a customer, in anonymous or fictitious / benami name(s) / entity (ies).
b. The Company shall accept customers only post verification and establishing the identity of the customer and its beneficial owner(s), if any.
c. No transaction and / or account shall be opened/ closed without effecting Customer Due Diligence Procedures laid down under this policy. All necessary processes are to be implemented, before opening an account, to ensure that the identity of the customers does not match with any person with known criminal background or who is associated with known criminal organizations such as individual terrorists or terrorist organizations etc.
d. The Company shall strictly not engage with customers and its beneficial owner(s), if any, having criminal background / are included in the negative / sanctions lists issued by regulators.
e. The Customer, for the purposes of acceptance for account based relationship / financial transaction, shall be identified at the Unique Identification Code level.
f. In case of Joint Account Holders, Company shall ensure that Customer Due Diligence Procedures are undertaken for all joint holders before opening an account.
g. 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 and instructions.

h. The company shall not open an account or close an existing 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.

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

j. The decision to open an account / enter into a transaction with Politically Exposed Persons ["PEP"] shall be taken solely at the level of the Board of Directors. It may however, be necessary to have suitable built in safeguards shall be provided to avoid any harassment to 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.

k. The Company shall classify the proposed customer into the prescribed risk categories, based on the risk perception under the Client Identification Procedures. On the basis of risk perception, the Company shall apply acceptance criteria for each category of customers.

l. The company shall list down circumstances in which a customer is permitted to act on behalf of another person/entity is clearly laid down 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.

m. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

n. Where an equivalent e-document is obtained from the customer, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

11. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

Customer Identification means identifying the Customer and verifying his/her/its identity by using reliable, independent source documents, data or information. The 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. The requirement as mentioned herein may be moderated according to the risk perception for e.g. in the case of a public listed company it may not be necessary to identify all the shareholders. Decision- making functions of determining KYC norms shall not be outsourced for according sanction for credit facilities, if any. The company shall for the purpose of verifying the identity of the customers at the time of an account-based relationship, rely on due diligence done by a third party subject to the outsourcing policy of the company and the following conditions:

a. The records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or C-KYC Records Registry.

b. Adequate steps shall be taken by the company to satisfy themselves that the copies of identification data and other relevant documentation relating to customer due

diligence requirements shall be made available from the third party request without delay.

c. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with requirements and obligations under PML Act.
d. The third party shall not be based in a country or jurisdiction assessed as high risk.
e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable with the company.

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 ident ity 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
c. Understand the ownership and control structure of the customer and determine who are the natural persons ultimately controlling 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.

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 ten years in case of Low Risk Category Customers and once in two years in case of High and once in every eight years for Medium Risk Categories as per the following procedure:

i. The company shall carry out PAN verification from the verification facility available with issuing authority.
ii. Authentication, of Aadhaar number already available with the company with the explicit consent of the customer.
iii. In case identification information available with Aadhaar does not contain current address as OVD containing current address may be obtained.
iv. Certified Copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized as low risk. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self - certification to that effect shall be obtained. Res shall ensure KYC documents are available with them.
v. The company may not insist on the physical presence of the customer for the purpose of

furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that the physical presence of the holders is required to establish their bonafide.

vi. The company shall provide acknowledgement with date of having performed KYC updation.

vii. The time limits prescribed would apply from the date of last verification of KYC.

12. CUSTOMER DUE DILIGENCE (CDD) PROCEDURES

Procedure for obtaining Identification Information

The company shall obtain the following information from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

a) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number where,

i) he decides to submit his Aadhaar number voluntarily Company notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address;

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the company:

Provided that where the customer has submitted,

ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the company shall carry out offline verification.

iii) an equivalent e-document of any OVD, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the company shall carry out verification through digital KYC as specified under Annex I.

Provided that for a period not beyond such date as may be notified by the Government for a class of company, instead of carrying out digital KYC, the company pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

b) From an individual who is not eligible to be enrolled for an Aadhaar number, or who is not a resident, the following shall be obtained

i. PAN or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time.
ii. one recent photograph and
iii. A certified copy of an OVD containing details of identity and address.

Provided that in case the OVD submitted 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.

While opening accounts of legal entities as specified in case, PAN of the authorized signatory or the power of attorney holder is not submitted, the certified copy of OVD of the authorized signatory or the power of attorney holder shall be obtained, even if such OVD does not contain address.

c) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have current address, an OVD as defined above shall be obtained from the customer for this purpose.

"Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by
iv. 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;

Provided further that the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents"

d) The company shall at the time of receipt of the Aadhaar Number shall carry out with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.

Provided,

i. Yes/No authentication shall not be carried out while establishing an account based relationship.

ii. In case of existing accounts where Yes/No authentication is carried out, REs shall ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/no authentication.

iii. Yes/No authentication in respect of beneficial owners of a legal entity shall suffice in respect of existing accounts or while establishing an account based relationship.

iv. Where OTP based authentication is performed in 'non-face to face' mode for opening new accounts, the limitations as specified in Section 17 shall be applied.

v. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators/ Biometric enabled ATMs.

e) In case the customer eligible to be enrolled for Aadhaar and obtain a Permanent Account Number, referred to in Section 15(a) above, does not submit the Aadhaar number or the Permanent Account Number/ form 60 at the time of commencement of an account-based

relationship with a RE, the Customer shall submit the same within a period of six months from the date of the commencement of the account- based relationship. In case the customer fails to submit the Aadhaar number or Permanent Account Number/form 60 within the aforesaid six months period, the said account shall cease to be operational till the time the Aadhaar number and Permanent Account Number/form 60 is submitted by the customer. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

f) The Company shall dully inform the customer about this provision while the opening the account.

g) The customer, eligible to be enrolled for Aadhaar and obtain the Permanent Account Number, except one who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, already having an account-based relationship with REs, shall submit the Aadhaar number and Permanent Account Number/ form 60 by such date as may be notified by the Central Government. In case the customer fails to submit the Aadhaar number and Permanent Account Number/form 60 by such date, the said account shall cease to be operational till the time the Aadhaar number and Permanent Account Number/form 60 is submitted by the customer.

The company shall apply the following procedure while establishing an account-based relationship:

a) Obtain information as mentioned under section 15 of KYC directions as applicable
b) Such other documents pertaining to the nature of business or financial status specified by the company in their KYC Policy.

Information collected from the customers shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling or for any other purpose without the express permission of the customer.

An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure II.

Accounts opened using OTP based E-KYC in non - face to face mode are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP
ii. the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete
iii. the aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.
iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year
v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
vi. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits

shall be allowed.

vii. The company shall ensure that only one account is opened using OTP based KYC in non-face to face mode and a declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face to face mode. Further, while uploading KYC information to CKYCR, REs shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face to face mode.

viii. The company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

REs may undertake V-CIP to carry out:

i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

ii. Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28, apart from undertaking CDD of the proprietor.

iii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

iv. Updation/Periodic updation of KYC for eligible customers.

REs opting to undertake V-CIP, shall adhere to the following minimum standards:

a) V-CIP Infrastructure

i. The RE should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the RE and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii. The RE shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv. The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii. The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

b) V-CIP Procedure

1. Company shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
2. If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.
3. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
4. Any prompting, observed at end of customer shall lead to rejection of the account opening process.
5. The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.
6. The authorised official of the company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
    i. OTP based Aadhaar e-KYC authentication
    ii. Offline Verification of Aadhaar for identification
    iii. KYC records downloaded from CKYCR, in accordance with Section 56 of RBI circular, using the KYC identifier provided by the customer
    iv. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of RBI circular

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Company shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Company shall ensure that no incremental risk is added due to this.

7. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
8. Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.
9. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
10. The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
11. Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.
12. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.
13. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the RE.

C) **V-CIP Records and Data Management**

i. The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

ii. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

Simplified Procedures for opening accounts by Non-Banking Finance Companies

In case the customer is not able to produce identification information, the company may with the approval of Board of Directors open accounts subject to the following conditions:

a. The company shall obtain a self-attested photograph of the customer

b. The designated officer of the company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence
c. The account shall remain operational initially for a period of twelve months within which the customer has to furnish identification information
d. The identification process is to be completed for all the existing accounts opened on such basis within a period of six months
e. Balance in all their accounts taken together shall not exceed rupees fifty thousand at any point of time
f. Total credit in all accounts taken together shall not exceed one lakh rupees a year
g. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed
h. The customer shall be notified when the balance reaches Rupees Forty Thousand or the total credit in a year reaches Rupees Eighty Thousand that appropriate documents for conducting KYC must be submitted otherwise the operations in the account shall be stopped.
i. Unique Customer Identification Code

   The Company shall assign a Unique Customer Identification Code ["UCIC"] to both existing as well as new customers, in order to link all account-based relationships / transactions to the customer. KYC verification once done by one branch/office of the RE shall be valid for transfer of the account to any other branch/office of the same RE, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

13. RISK MANAGEMENT

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 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.

The Customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes other than for disclosure of events / transactions to the Credit Information Companies, based on the Company's agreement with the Credit Information Companies.

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.

A. High Risk – Category A Customers

High Risk Customers typically include:

1) Non-Resident Customers
2) High net worth individuals without an occupation track record of more than 3 years
3) Trust, charitable organizations, Non-Government Organization (NGO), organizations receiving donations
4) Companies having close family shareholding or beneficial ownership;
5) Firms with sleeping partners
6) Politically exposed persons (PEPs) of Indian/ foreign origin;
7) Non Face to face Customers
8) Person with dubious reputation as per public information available.

B. Medium Risk – Category B Customers

Medium Risk Customers typically include:

1) Salaried applicant with variable income/ unstructured income receiving Salary in cheque
2) Salaried applicant working with Private Limited Companies, Proprietary, Partnership firms
3) Self- employed professionals other than High Net-Worth Individuals
4) Self-employed customers with sound business and profitable track record for a reasonable period
5) HNIs with occupation track record of more than 3 years

C. Low Risk – Category C Customers

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:

1) Salaried employees with well-defined salary structures for over 5 years
2) 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 approval from Board of Directors in such cases to continue the business relationship with such person, and also undertake enhanced monitoring as indicated and specified in Annexure I .
3) People belonging to lower economic strata of the society whose accounts show small balances and low turnover
4) People working with Public Sector Units
5) People working with reputed Public Limited Companies and Multinational Companies

The Management of the Company under the supervision of the Board of Directors shall ensure that an effective KYC procedure is put in place by establishing appropriate processes and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility is to 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.

14. 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 endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular pattern of activity can be identified. Special attention is to 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 are to be subjected to intense monitoring. Company shall set key indicators for such accounts based on 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. The 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 but not limited to RBI watch list.

15. TRAINING PROGRAMES

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. The front desk staff shall be specially trained to handle issues arising from lack of customer education. The company shall have a proper staffing of the audit function with persons adequately trained and well- versed in AML/CFT policies of the company, regulations and the related issues.

16. INTERNAL CONTROL SYSTEM/SOFTWARE

The Company's Internal 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 Board of Directors shall ensure that the audit function is staffed adequately with skilled individuals. It is essential to specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as t o ensure that person of criminal nature/ background do not get an access, to misuse the financial channel. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions. AML Software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions with customers.

17. RECORD KEEPING

The company shall take the following steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules:

a. Maintain all necessary records of transactions between the company and the customer, both domestic and international for at least five years from the date of transaction

b. Make available the identification records and transaction data to competent authorities upon request

c. Ensure a proper system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules,2005

d. Maintain all necessary information in respect of transactions prescribed in Rule 3 of PML Rules:
   - 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
   - the parties to the transaction, especially the documents for identification of beneficial owner

The Company shall maintain proper records 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 Lakhs (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 Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees Ten Lakh or its equivalent in foreign currency.

c. All transactions involving receipts by non-profit organizations of Rupees ten lakhs or its equivalent in foreign currency

d. All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions

e. All cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of the fund is in India

f. All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity as the case may be.

g. 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 III

18. REPORTING ON FINnet PORTAL AND REPORTING TO FINANCIAL INTELLIGENCE UNIT- INDIA

Reporting on FINnet Portal

The company shall furnish to the director, the Financial Intelligence Unit – India (FIU-Ind) information referred to in Rule 3 of PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. The company shall take note of reporting formats and comprehensive reporting formatting guide prescribed/released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in preparation of prescribed reports. The Company shall register on the FINnet portal, alongwith undertaking registration of the Principal Officer. The reports shall be filed by the Company online only. Any change in the Principal Officer shall be effected on the FINnet portal by the Company within one month of the date of such change. The Principal officers of the company, where branches are not fully computerized, shall have a suitable arrangement to cull out the transaction details from branches which are not yet computerized.

Reporting to Financial Intelligence Unit – India (FIU-Ind)

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

The Director,
Financial Intelligence Unit – India,
06th FloorTower-2,
Jeevan Bharati Building,
Connaught Place,
New Delhi-110001, INDIA.

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

19. CENTRAL KNOW YOUR CUSTOMER REGISTRY

The Company shall register itself on the Central Know Your Customer Registry ["CKYCR"] maintained by Central Registry of Securitisation and Asset Reconstruction and Security Interest of India ["CERSAI"] for the purposes of sharing KYC data. The Company shall ensure that the KYC data is regularly shared / verified from the CKYCR.

Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

The Company shall nominate two officers as 'Compliance Officers' for the purpose of holding the roles of User Administrators. The two compliance officers so appointed shall function in a manner wherein the maker checker concept amongst them is followed.

20. CERSAI

The Company shall register itself on CERSAI, and shall share all relevant information required, relating to the equitable mortgages created in the favor of the Company.

21. OUTSOURCING

The Company, in normal operating conditions, shall not outsource its financial activities. However, under circumstances of operational stress, the Company may outsource procedures relating to KYC / AML / CFT, subject to specific approval of the Board of Directors. However, such outsourcing shall be limited to compilation / collection of documentation and / or physical verification / visits, as may be required.

The decision-making process for sanction of a credit proposal or otherwise and determining compliance with KYC norms shall solely rest with the Company and shall strictly not be outsourced. The risk categorization of a loan proposal shall also be undertaken by the Company, and shall not be outsourced.

22. REPORTING REQUIRMENT UNDER FOREIGN ACCOUNT TAX COMPALIANCE ACT (FATCA) AND COMMOR REPORTING STANDARDS (CRS)

The company shall adhere to the provisions of Income Tax Rules to determine the applicability of being a Reporting Financial Institution and comply with the reporting requirements.

23. GENERAL

a) Customer Education

Company shall educate Customers on the objectives of the KYC policy 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 this policy.

b) 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 favor 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 proper banking channels and not against cash payment.

c) 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 due notice to the Customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of a Director and/or key managerial persons authorized for the purpose.

d) KYC for 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.

e) Updation in KYC Policy of Company

PO shall, after taking the due approval from the Board of Directors, make the necessary amendments / modifications in the KYC 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, but not later than once in a financial year.

24. E-KYC

The Company may undertake KYC process in electronic format as OTP based e -KYC for on boarding of customers, utilizing the e-KYC service of Unique Identification Authority of India (UIDAI), subject to following conditions:

- There must be a specific consent from the customer for release of identity through biometric authentication and authentication through OTP
- Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- Accounts, on account of borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure as provided in section 16 or as per the first proviso of Section 17 of the KYC Master Direction is to be completed. If the CDD procedure is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC either with the same company or with any other company. Further, while uploading KYC information to CKYCR, REs shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure.
- The Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above- mentioned conditions.

The Company shall print/download directly, the prospective customer's e -Aadhaar letter from the UIDAI portal, if such a customer knows only his/her Aadhaar number or if the cust omer carries only a copy of Aadhaar downloaded from a place/source elsewhere, provided, the prospective customer is

physically present at the place of business of the Company.

Exceptions to this Policy must be approved by the Chief Compliance Officer, or the designated person. All exceptions must be documented, with reasons for the exceptions, including expiration or review date and, wherever necessary, include an action plan and timelines for compliance with the Policy.

25. EXPCEPTION HANDLING

Exceptions to this Policy must be approved by the Chief Compliance Officer, or the designated person. All exceptions must be documented, with reasons for the exceptions, including expiration or review date and, wherever necessary, include an action plan and timelines for compliance with the Policy.

26. EFFECTIVE DATE

This policy has been adopted vide Company's Board of Directors' resolution dated **25th August, 2016**. This policy shall stand applicable organization wide with effect from 25th August, 2016.

This policy or any of its clauses are to be suitably modified based on the Directions of Reserve Bank of India from time to time and shall be put before the Board of Directors in their meeting immediately succeeding such changes/amendments.

-X-X-X-X-

Annexure I

Customer Identification Requirements

1. 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 provide financial services to an account for PEP shall be taken at the Board of Directors 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.

2. Accounts of non-face-to-face Customers

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 mitiga te the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of cross -border Customers, there is the additional difficulty of matching the Customer wit h the documentation and the Company 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.

3. Trust/Nominee or Fiduciary Accounts

The Company 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 Perso ns 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 set tling 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.

4. Accounts of companies and firms

The Company needs to be vigilant against business entities being used b y individuals as a front for maintaining accounts with the Company. The Company mandatorily has to 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 public company it shall not be necessary to identify all the shareholders.

Know Your Customer (KYC) Process

Client Registration Form for each client shall be obtained before opening an account.

Mandatory Documents:

Collect the relevant documents, supporting and proofs as per documentation requirements established in the organisation.

Verification and Due diligence by KYC Desk

a. KYC desk to receive duly filled in Client Registration Docket along with the supporting documents from Relationship Manager (RM) and to verify duly filled Client Registration Docket with the supporting documents for their completeness in all respects and to rectify the same in case of any deficiencies.

b. Ensure that all the supporting documents and other additional documents are collected and are self-attested by the client himself.

c. In case of Corporate clients, ensure that Resolution of Board of Directors approving the transactions and naming the authorized persons for carrying out the necessary formalities on letter head of the company.

d. Ensure that corporate client is authorized to enter into loan transaction and carry out the activity for which the loan is being taken as per Memorandum of Association and Articles of Association and should be marked by RM.

e. While interacting with the Client, RM/KYC desk may conduct due diligence of the client for knowing the client's background, history, financial status / capability, assessment of business patterns and to verify genuineness of the client.

f. Cross check PAN details of the client like Permanent Account Number, Name, Father's Name (in case of Individual client), Date of Birth / Incorporation with the de tails on the website of the Income Tax Department and attach the proof of the same with KYC docket.

g. In case PAN details are not matching substantially with PAN details printed on PAN Card and PAN details appearing on IT website, take appropriate action to get it clarified from the client. In case of minor discrepancy in the name, obtain the declaration from the client about the same.

h. Ensure that name filled up in client registration form, Agreement and other document is same as name appearing on PAN card.

i. KYC desk should check 'world-check.com', 'watchoutinvestors.com' and SEBI/ Exchange website for client's history and status.

j. In case of a corporate client, ensure that the name of the company is not appearing in the list of vanishing companies as provided on Ministry of Corporate Affairs (MCA) website. Keep the checking detail with the KYC docket.

k. In case of default or any action taken by any regulatory authorities against such client is found on verification then seek clarification from the client and co -ordinate with client or RM to find out further details in such default and status as on date.

l. Check the details of prospective client/customer in CIBIL records for defaults as appearing in the records.

m. Dispatch welcome letter stating details like Client code allotted, his email ID, important terms and conditions of the contract and loan facility offered etc. to the client as per fair practice code and maintain the dispatch records.

n. A copy of all the documents executed by client shall be given to him, within reasonable time from the date of acceptance of loan request. Client acknowledgement shall be obtained for receipt of the same.

Due Diligence from PMLA Point of view

a. Customer Identification Procedures shall be applied to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transactions involved.

b. Company shall determine from available sources of information whether the client or potential client or the beneficial owner of such client is a politically exposed person (PEP).

c. Company shall obtain sufficient information in order to identify persons who beneficially own or control or influences a client's loan account. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

d. Whenever it is apparent that the loans account maintained is beneficially owned by a party other than the client, that party will be identified using client identification and verification procedures.

e. Company shall apply customer due diligence on a risk sensitive basis depending on the type of customer, business relationship or transaction.

f. Documentation requirement and other information will be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement of the PMLA, guidelines issued by RBI from time to time. Indicative list for additional documents that may be obtained from High Risk Clients:

- Annual Statement of the accounts / financial information
- Sources of Funds / Securities (if any),
- Last 6 months bank statements,
- Last 6 months demat transactions statements, etc.
- Employment / Profession Status and Certificate thereof,
- Group Company / other relatives details,
- It shall be ensured that a loan account is not opened where the Company is unable to apply appropriate clients due diligence measures / KYC policies.
- Where it is not possible to ascertain the identity of the client,
- Information provided to the intermediary is suspected to be non-genuine,
- There is perceived non co-operation of the client in providing full and complete information

g. Necessary checks are to be in place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide. (For e.g. list of individuals/entities as obtained from United Nations website should be checked, The Company before opening any new account will ensure that the name/s of the proposed customer/client does not appear in the list.

h. Necessary checks also to be conducted for existing clients on ongoing basis to ensure that they are not falling in banned list provided by stock exchanges / SEBI / RBI from time to time.

The KYC information obtained shall be shared with the Central KYC Records Registry in the manner mentioned in the Rules, as required by the KYC templates available for 'Individuals' and 'Legal Entities', as the case may be.

Client Acceptance and Identification Process

a. The Company has to ensure that the existing guidelines regarding Customer / business acceptance is strictly followed. Existing / past relationship with the client should be verified and ensured that the client is not on the negative list / defaulters list.

b. A detailed search to be carried out to find that the Client is not in defaulters / negative list of regulators. (Search should invariably be carried out on SEBI website www.sebi.gov.in, CIBIL website www.cibil.com, relevant data received from CIBIL, sanctions list issued by Reserve Bank of India and Ministry of Company Affairs sponsored website www.watchoutinvestors.com.)

c. In case of corporates, the antecedents of the company (change of name and registered office in particular) and of all promoters and directors is to be traced.

d. In case of need, an opinion report may be obtained from the bankers / institutions financing the client.

e. An assessment shall be made of the financial worthiness of the client by obtaining appropriate declarations at KYC stage.

f. A thorough assessment shall be carried out to ascertain whether the client is dealing with the company on his own behalf or someone else is the beneficial owner. If there are doubts, before acceptance of the clients, thorough due diligence shall be carried out to establish the genuineness of the claims of the clients. Secrecy laws shall not be allowed as a reason to disclose true identity of the beneficiary / transacting party.

g. No client shall be accepted where it is not possible to ascertain the identity of the client, or the information provided is suspected to be non-genuine, or if there is perceived non- cooperation of the client in providing full and complete information. The company shall not continue to do business with such a person and file a suspicious activity report. The company shall consult the relevant authorities in determining what action it shall take when it suspects suspicious transactions being carried out.

h. No transaction or account based relationship is to be undertaken without following the Customer Identification Procedures.

i. In the case of Clients who want to act through agent under Power of Attorney, a notarized power of attorney shall be obtained along with request letter from the client, proof of identity and address of power of attorney holder. Original of the POA and identity, address proof should be verified. Care should be taken to ensure the genuineness of the client and his agent.

j. Know Your Client forms duly signed by the client shall be obtained before acceptance of the clients.

k. In case the client belongs to CSC (Client of Special category), the additional due diligence process shall be initiated.

l. Any transaction from the client shall be accepted only after customer acceptance procedure is completed.

The following categories will be deemed to be special category clients

Non-resident clients

High Net worth clients

Trust, Charities, NGOs and organizations receiving donations

Companies having close family shareholdings or beneficial Ownership

Politically exposed persons (PEP) of foreign origin 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.

Family members or close relatives of PEPs

Current or Former Senior High profile politicians and connected persons (imme diate family, Close advisors and companies in which such individuals have interest or significant influence)

Companies offering foreign exchange offerings

Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.

Non face to face clients

Clients with dubious reputation as per public information available etc. (checking can be done on SEBI, RBI, Exchange, Watchoutinvestors.com, 'Worldcheck', 'Google' check, etc. website to categorized the client)

Any other category of client as may be defined and included by the company under this list or on a case to case basis from time to time.

Client identification procedures shall be carried out at following different stages:

While establishing the relationship with the client

While carrying out transactions for the client

When the company has doubts regarding the veracity or the adequacy of previously obtained client identification data.

The Company shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relations hip. Each original document shall be seen prior to acceptance of a copy. The authorised persons' signature has to be obtained on the KYC kit stating "All Originals seen and verified" and also stamped of in -person verification by the employee of the company.

Failure/Refusal by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the Company.

Risk based approach shall be followed towards certification of documentation.

Identification of client and introduction by an acceptable person are important pre -requisite for opening an account. Proper introduction or verification of the identity of the client may be obtained while opening an account.
Before opening the accounts, a personal interaction may be had with the client except in the case of NRIs where the power of attorney holder is the Authorised dealer Bank.

In case of companies, any one of the following viz. main promoter/ Managing Director/ whole time director / key management person and in the case of partnership any one of the active partners may be met in person before opening the loan accounts.

Caution is to be exercised when identifying companies which appear to be 'shell companies' or 'front companies'. Shell/front companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted.

After opening the account, a letter of thanks / welcome letter should be sent by registered post/speed post, at the recorded address. This will serve the dual purpose of thanking them for opening the account and for verification of genuineness of address provided by the account holder. Transactions should not be allowed if the mail comes undelivered. The undeliver ed envelope should be retained with the KYC papers for further inquiries, if necessary.

KYC Rejection Procedures

In case where the documents or information obtained from client is not sufficient as outlined in the policy, the KYC will be rejected unless it is covered under the exception handling procedure as mentioned above. Any changes/amendments made in the Policy shall be put before the Board of Directors in their meeting immediately succeeding such changes/amendments, for purpose of information.

X-X-X-X

Annexure II

Indicative List of Documents to be obtained for Client Identification Procedures

Features	Documents
Accounts of Individuals - Legal name and any other names used and Correct permanent address	a. Aadhaar Card b. PAN card(Mandatory) c. Passport d. Voter's Identity Card e. Driving license f. Identity card (subject to the Company's satisfaction) g. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank h. Telephone bill i. Bank account statement j. Letter from any recognized public authority k. Electricity bill l. Ration card m. Letter from employer (subject to satisfaction of the bank) (any one document form c to m above which provides customer information to the satisfaction of the company will suffice)

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. Copy of PAN allotment letter e. Copy of the telephone bill f. Officially Valid Documents of the Power of Attorney holder

Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	a. Registration certificate, if registered b. Partnership deed c. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf d. Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses e. Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	a. Certificate of registration, if registered b. Power of Attorney granted to transact business on its behalf c. Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses d. Resolution of the managing body of the foundation/association e. Telephone bill f. Electricity Bill g. Trust Deed h. Copy of PAN

X-X-X-X

Annexure III

Illustrative List of Suspicious Transactions

Suspicious Activities 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.

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.

Activities not consistent with the Customer's Business

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

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 a 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.

Unusual Activities

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

Customer/Client 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 fre quent large transactions.

Employees arousing Suspicion

An employee whose lavish lifestyle cannot be supported by his or her salary.

Negligence of employees/wilful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored:

Large Cash Transactions

Multiple accounts under the same name

Placing funds in term Deposits and using them as security for more loans

Sudden surge in activity level

Same funds being moved repeatedly among several accounts

X-X-X-X