KNOW YOUR CUSTOMER (KYC) &
PREVENTION OF MONEY LAUNDERING (PMLA) POLICY

AEFPL

Arthashastra Fintech Private Limited

V.1 updated in June, 2022

PREAMBLE:

The Reserve Bank of India (RBI) has issued comprehensive Master Direction - Know Your Customer (KYC) Direction, 2016 to all Regulated Entities (REs) including Non-Banking Financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and 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, Arthashastra Fintech Private Limited ("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 of Directors.

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 risks 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 risks prudently;

3. To put in place 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 nine (9) key elements:

    a) Customer Acceptance Policy (CAP);
    b) Customer Identification Procedures (CIP);
    c) Monitoring of Transactions;
    d) Risk Management;
    e) Training Programme;
    f) Internal Control Systems;
    g) Record Keeping;
    h) Appointment of Principal Officer;

i) Reporting to FIU – India.

DEFINITION OF CUSTOMER:

For the purpose of Company's KYC policy, a 'Customer' means a Person who is engaged in a financial transaction or activity with the company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

A "Person" shall have the meaning as defined under KYC Directions issued by RBI (and any amendment from time to time by RBI) which at present is as follows:

'Person' shall include:

(i) an Individual;

(ii) a Hindu Undivided Family;

(iii) a Company;

(iv) a Firm;

(v) an association of persons or a body of individuals, whether incorporated or not;

(vi) every artificial juridical person, not falling within any one of the above persons (i to v);

(vii) any agency, office or branch owned or controlled by any one of the above persons (i to vi).

KEY ELEMENTS:

I. Customer Acceptance Policy ("CAP"):

1. 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 is opened in anonymous or fictitious / benami name.

b) No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

c) No transaction or account-based relationship is undertaken without following the CDD procedure.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

e) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

f) CDD Procedure is followed for all the joint account holders, while opening a joint account.

g) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

h) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

i) Apply CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.

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

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

2. The Company shall prepare a profile for each new Customer during the credit appraisal based on risk categorization. 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. Any other information from the Customer should be sought separately with his/her consent and after opening the Registered 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, unless specifically authorized by the customer to do so.

3. 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.

4. (i) 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 foreign origin;

g) Non-Face to face Customers;

h) Person with dubious reputation as per public information available;

(ii) 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;

(iii) 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;

II. Customer Identification Procedures ("CIP"):

1. 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. 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.

2. 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,

Date of Birth and also his recent photograph. For customers that are legal persons or entities, the Company shall;

i) verify the legal status of the legal person/ entity through proper and relevant documents;

ii) 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,

3. Ultimate Beneficial Owner (UBO): 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.

4. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is also 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.

5. 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 ten years in case of Low Risk Category Customers, once in two years in case of High-Risk customers and once in every eight years for Medium Risk Customers.

III. 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 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.

IV. 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.

V. 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.

VI. 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.

VII. Record Keeping:

1. 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 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.

   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 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.

2. 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.

3. 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 Five (05) years from the date of transactions between the customers and Company.

records of the identity of all Customers of Company are required to be maintained for a period of Five (05) years from the date of cessation of transactions between the Customers and Company.

b) 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.

VIII. 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. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT.

IX. Reporting to Financial Intelligence Unit – India:

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

http://fiuindia.gov.in

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

X. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR):

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rule, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. 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.

XI. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, NBFC shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and shall register itself with with Income Tax Department. The company shall submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report by May 31 of each year.

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 desk 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 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 cheques and not against cash payment.

III. 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/ 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)

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.
   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 and to accounts where a PEP is the beneficial owner

2. 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.

3. Accounts of companies and firms:

   Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining 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 e.g. in the case of a public company it shall not be necessary to identify all the shareholders.

4. Accounts opened by professional intermediaries:

Customer accounts opened by professional intermediaries when the branch/office has knowledge or reason to believe that the Customer account opened by a professional intermediary is on behalf of a single Customer, that Customer must be identified. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branch/office also maintain 'pooled' accounts managed by lawyers/ chartered accountants for funds held 'on deposit' for a range of Customer. Where funds held by the intermediaries are not co-mingled at the branch/office and

there are ‘sub-accounts’, each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the branch/office, the branch/office shall still look through to the beneficial owners. Where the branch/ office rely on the ‘Customer Due Diligence’ (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the Customer lies with the branch/office.

ANNEXURE II

Customer Due Diligence Procedure Features to be verified and Documents that may be obtained from Customers:

1. Individuals (Applicant/ Co – Applicant):

Customers, at their option, shall submit one of the following Officially valid document (OVDs) for proof of identity and proof of address and One recent photograph.

(a) the Aadhaar number where,

he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or he decides to submit his Aadhaar number voluntarily to a bank or any RE 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; and

(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 like the passport, the driving license, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. 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 RE:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank or to a RE notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or RE shall carry out authentication of the customer’s Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.

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

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; the customer shall submit OVD with current address within a period of three months of submitting the documents.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmityon account of old age or otherwise, and similar causes, REs shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer.

Note: RE shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

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.

A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account-based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

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

There must be a specific consent from the customer for authentication through OTP.

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.

Accounts opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out..

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 with any other RE. 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.

REs may undertake live V-CIP, to be carried out by an official of the RE, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the RE performing the V-CIP shall record video as well as capture photograph of the customer present for identification. However, REs other than banks: can only carry out Offline Verification of Aadhaar for identification.
ii. RE 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the RE shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the RE shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. 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.

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the REs shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. REs are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.

xiii. RE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

xiv. BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. 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.

2. Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

a. Registration certificate
b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. [33]CST/VAT/ GST certificate (provisional/final).
e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
h. Utility bills such as electricity, water, landline telephone bills, etc

In cases where the REs are satisfied that it is not possible to furnish two such documents, REs may, at their discretion, accept only one of those documents as proof of business/activity.

3. Legal Entities

(3A) For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Certificate of incorporation
b. Memorandum and Articles of Association
c. Permanent Account Number of the company
d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
e. Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

(3B)For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate
b. Partnership deed
c. Permanent Account Number of the partnership firm
d. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

(3C) For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate
b. Trust deed
c. Permanent Account Number or Form No.60 of the trust
d. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

(3D) For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Resolution of the managing body of such association or body of individuals
b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
c. Power of attorney granted to transact on its behalf
d. Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
e. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

ANNEXURE III

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTION PERTAINING TO FINANCIAL SERVICES

"Suspicious transaction" is defined in PMLA rules as 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.

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:

   a) 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 favor 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.