

Equentia Financial Service Private Limited

Know Your Customer (KYC) and Prevention of Money Laundering (PMLA) Policy

CRED^{ABLE}™

Document Management:

Document Name	KYC-AML Policy
Original Document Date	V 1.0 dated January 18, 2019
Review Version & Date	V 1.1 dated June 24, 2019
Next Review by Board of Directors	29 th November 2019
Next Review by Board of Directors	23 rd June, 2020
Last review by Board of Directors	20 th Februarys, 2025
Last review by Board of Directors	19 th August, 2025

Know Your Customer (KYC) and Prevention of Money Laundering (PMLA) Policy

Table of Contents

1. Preamble.....	3-3
2. Background & Objective.....	3-5
3. Definitions.....	5-9
4. Appointment Of Designated Director.....	9-9
5. Appointment Of Principal Officer (PO)	9-9
6. Compliance Of KYC Policy.....	10-10
7. Money Laundering and Terrorist Financing Risk Assessment.....	11-11
8. Key Elements of the KYC Policy.....	11-27
15. Annexure – I.....	28-30
16. Annexure - II.....	31-37
17. Annexure - III.....	38-39
18. Annexure - IV.....	40-48
19. Annexure - V.....	49-50
20. Annexure - VI.....	50-50

PREAMBLE

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all 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. In view of the same, AFSL has adopted the said KYC guidelines with suitable modifications depending on the business activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures be formulated in line with the prescribed RBI guidelines and put in place duly approved by its Board of Directors.

As a result, Equentia Financial Services Private Ltd ("EFSPL" or "CredAble" or the "Company") has framed and adopted the Policy of Know Your Client and Prevention of Money Laundering (the 'Policy'), as approved and reviewed by the Board from time to time, covered in this document. This Policy may also be referred to as KYC-AML guidelines or KYC-AML Policy or KYC-PML guidelines or KYC-PML Policy by the Company in this and all other document unless otherwise specifically defined.

Since the RBI Master Direction – Know Your Customer (KYC) Direction, 2016 Ref. No. DBR.AML.BC. No.81/14.01.001/2015-16 dated February 25, 2016, updated from time to time and last updated on November 06, 2024, to align with the recent amendments carried out in Prevention of Money Laundering Act, 2002 and Prevention of Money Laundering (Maintenance of Records) Rules, 2005, this Policy is required to be updated.

In view of the above, the Board of Directors have reviewed and approved the existing Policy which has been updated by incorporating the latest RBI guidelines and provisions of the PML Rules and Act.

BACKGROUND & OBJECTIVE

Money laundering refers to concealing or disguising the origin and ownership of the proceeds from criminal activity, including drug trafficking, public corruption, terrorism, fraud, human trafficking, and organized crime activities. Terrorist financing is the use of legally or illegally obtained funds to facilitate terrorist activities. Money laundering and terrorist financing may involve a wide variety of financial products, services, and transactions including lending and investment products, and the financing of equipment and other property that could be used to facilitate terrorism and other criminal activity.

Generally, the money laundering process involves three (3) stages: placement, layering and integration. As illegal funds move from the placement stage through the integration stage, they become increasingly harder to detect and trace back to the illegal source.

- 1) Placement is the point where illegal funds first enter the financial system.
- 2) Layering After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.
- 3) Integration occurs when the criminal believes that there are sufficient number of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

To prevent money-laundering in India and to provide for confiscation of property derived from, or involved in, money-laundering and related matters, the Parliament of India enacted the Prevention of Money Laundering Act, 2002 (PMLA), as amended from time to time. Further, necessary Notifications / Rules under the said Act have been published and amended by the Ministry of Finance, the Government of India.

As per the Prevention of Money Laundering Act 2002, the offence of Money Laundering is defined as: *"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."*

The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime. The Reserve Bank of India (RBI) vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25 2016 and subsequent modifications thereof, have prescribed guidelines "Anti Money Laundering" guidelines/ standards.

In view of the above, KYC-AML policy of the Company has been framed to broadly achieve the following purposes:

- a) To prevent criminal elements from using the Company for money laundering activities;
- b) To enable Company to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
- c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
- d) To comply with applicable laws and regulatory guidelines;
- e) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. P

Applicability:

This Policy will be applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time.

Branch/Office/majority owned subsidiaries located outside India:

If the Company has any branch/ office/ majority owned subsidiaries which are located outside India, this KYC-AML Policy shall be applicable to branch / office/ majority owned subsidiaries located outside India to the extent that they are not contradictory to the local laws in the host country, provided that:

- i. where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India. RBI may advise further necessary action by the Company including application of additional measures to be taken by the Company to manage the ML/TF risks.
- ii. in case there is a variance in KYC/AML standards prescribed by the Reserve Bank of India and the host country regulators, branches/ subsidiaries of Company are required to adopt the more stringent regulation of the two.

DEFINITIONS**1. Customer:**

The policy will be applicable to all “Customers” including Applicant, Co-Applicant, Guarantor, Beneficial Owner (BO), Business Partners. “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. Customer will include the following:

- a. an individual, p
- b. a Hindu undivided family,
- c. a company,
- d. a firm,
- e. an association of persons or a body of individuals, whether incorporated or not,
- f. every artificial juridical person, not falling within any one of the above persons (a to e), and
- g. any agency, office or branch owned or controlled by any of the above persons (a to f).

KYC documentation collection, its validation and OSV check/certification as specified in this policy shall be fulfilled either in physical form, V-CIP or in digital mode.

2. Beneficial Owner (BO):

in relation to a Customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the Customer. A list of persons who are to be considered as such BOs in relation to a Customer is given below:

Type of Customer	Persons to be considered Beneficial Owners (BOs)
In case of Company , the beneficial owner is the natural person(s), who, whether acting	(a) Controlling ownership interest – ownership of/entitlement to more than 10

alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.	percent of the shares or capital or profits of the Company; (b) Control shall include 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.
In case of 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 10 per cent of capital or profits of the partnership.	10 per cent of capital or profits of the partnership.
In case of unincorporated association or body of individual , 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.	More than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals or society.
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 10% 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.	10% or more interest in the trust

Notes:

- i. Term 'body of individuals' includes societies.
- ii. Where the **customer or the owner of the controlling interest is a company listed on a stock exchange**, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

- iii. Where no natural person is identified as per the above table, the beneficial owner is the relevant natural person who holds the position of senior managing official.

3. Transaction:

The policy will be applicable for all "Transactions" done by the company. "Transactions" means

A purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

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

4. Money Laundering:

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the "offence of money laundering" as under:

"Whose directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds or crime and projecting it as untainted property shall be guilty of offence of money laundering".

5. Customer Due Diligence (CDD):

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using 'reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

- (a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
- (b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
- (c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

6. Officially Valid Document (OVD):

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

Provided that,

- a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
 - 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.

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

7. Video based Customer Identification Process (V-CIP):

An alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

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

- a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to not have economic rationale or bona-fide purpose; or
- a.gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

9. Debarred Customers:

Debarred customers includes the customers whose names matches in RBI Defaulters’List, United Nations Security Council (UNSC), Financial Action Task Force (FATF), Office of Foreign Assets Control (OFAC), negative media searches, Politically Exposed Persons (PEPs).

Other terms not specifically defined here shall have the same meaning as assigned to them under the RBI’s KYC Directions, 2016 or Prevention of Money Laundering Act, as amended from time to time.

APPOINTMENT OF DESIGNATED DIRECTOR (DD)

As required by Reserve Bank, Mr. Nirav Choksi (DIN: 00906553), Executive Director has been appointed as Designated Director by the Board of Directors for ensuring compliance with the obligations under the PML Act. The name, designation address and contact details of the Designated Director including changes from time to time, shall be communicated to FIU-IND and RBI by Compliance/Secretarial Departments. Pursuant to this clause, Legal and Compliance Department shall separately notify the Designated Director with his roles and responsibilities under KYC and PMLA.

In no case, the Principal Officer shall be nominated as the Designated Director.

APPOINTMENT OF PRINCIPAL OFFICER (PO)

As required under the Prevention of Money Laundering Act, 2002 (PMLA), Mr. Ram Kewalramani (DIN: 00575917), Executive Director has been appointed as the Principal Officer of our Company. The Principal Officer shall *inter alia* be responsible for reporting for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the Prevention

of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time. The name, designation and address of the Principal Officer shall be communicated to FIU-IND and RBI by Compliance/Secretarial Department. Pursuant to this clause, Legal and Compliance department shall separately notify the PO with his roles and responsibilities under KYC and PMLA.

COMPLIANCE OF KYC POLICY

a) Constitution of Senior Management:

As per RBI circular, the Senior Management has been constituted for KYC Policy. Senior Management shall comprise of Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, Chief Human Resource Officer, Head of Business. The responsibility is for effective implementation of policies and procedures with their respective departments. Pursuant to this clause, Legal and Compliance department shall separately notify the Senior Management with its roles and responsibilities under KYC Policy.

b) Concurrent/Internal Audit:

Independent evaluation of the compliance functions pertaining to KYC and PMLA shall be done by Internal Audit Department. It would include the verification for compliance of KYC/AML policies and procedures (both design and implementation) on a quarterly basis and highlighting the necessary modifications if any so as to ensure the compliance. Compliance report on KYC Policy shall be submitted to Board or authorized Committee on quarterly basis.

c) Outsourcing:

Decision Making function of determining compliance with KYC Norm shall not be outsourced.

d) Hiring And Training:

Human Resource Department shall put in place the screening mechanism as an integral part of their personnel recruitment/hiring process. HR, Legal & Compliance and Operations Department shall arrange an on-going employee training program for the different categories of members of staff and ensure that they are adequately trained in KYC/AML procedures. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulation and related issues shall be ensured.

e) Customer Due Diligence:

Customer due diligence means identifying and verifying the customer and Beneficial Owner using “Officially Valid Documents” as proof of identity and a proof of address.

f) Central KYC Records Registry:

CKYCR means an entity to receive, store, safeguard and retrieve the KYC record in digital form of a customer. Operations Department has taken necessary steps to comply with the norms of

CKYCR within specified timelines. Government of India authorize the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

To have constant check over the risk posed due to money laundering and terrorist funding, Risk Assessment would be conducted by the Internal Audit Department (IAD).

- i IAD shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
- ii The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
- iii The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
- iv The outcome of the assessment shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.
- v The suggestion and mitigants confirmed by Board shall be implemented. IAD shall monitor the implementation of the controls and enhance them if necessary. Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, company shall monitor the implementation of the controls and enhance them if necessary.
- vi IAD would decide suitable process / procedural aspects by Chief Internal Auditor based on the above guidelines to implement the same.

KEY ELEMENTS OF THE KYC POLICY

The policy shall include following key elements:

- (i) Customer Acceptance Policy;
- (ii) Risk Management;
- (iii) Customer Identification Procedures (CIP) – (1) Physical, (2) Video – CIP, (3) Digital – KYC(specified in Annexure II and III);
- (iv) Customer Due Diligence (CDD) procedure as specified in Annexure IV and Business Partner Due Diligence;
- (v) Monitoring of Transactions;

- (vi) Training Programme;
- (vii) Internal Control System;
- (viii) Record Management;
- (ix) Reporting to Financial Intelligence Unit – India
- (xi) Central KYC Records Registry (CKYCR); and
- (xii) General;

CUSTOMER ACCEPTANCE POLICY

Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship with CredAble broadly are detailed below:

- a. No account shall be opened by the Company in anonymous or fictitious/benami names.
- b. No account is opened where the company is unable to apply appropriate Customer Due Diligence measures (CDD), 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 to be 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 shall be as specified in this procedure note.. Any exceptions shall be discussed / informed with the Principal Officer
- e. Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, is obtained with the explicit consent of the customer.
- f. The CDD procedure are applied at Unique Customer Identification Code level (UCIC).
- g. Accept customers only after verifying their identity, as per CDD Procedures defined aforesaid and shall be followed for all the joint account holders (including guarantors) as well, while opening a joint account. No Account shall be opened where the Company is unable to apply appropriate Customer due diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- h. In the event, the Customer is permitted to act on behalf of another person/entity, the Company shall verify that the Customer has the necessary authority to do so by scrutinizing the authorizing document/s. A suitable system will be 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. Such System's database should be updated periodically by Compliance and IT Team.
- i. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- j. 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.

- k. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- l. If the customer or the beneficial owner is PEP, then the same shall be specifically highlighted to the Principal Officer for their approvals.
- m. Implementation of CAP should not become too restrictive and result in denial of CredAble services to general public, especially to those who are financially or socially disadvantaged.
- n. 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 account.
- o. United Nations Security Council (UNSC) Lists: If the name of the customer entity/individuals appears on the 2 lists of individuals and entities, suspected of having terrorist links, no account shall be opened by the Company. The details of the 2 lists are as given below:
ISIL (Da'esh) & Al-Qaida Sanctions List
<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

1988 Sanctions List

<https://www.un.org/securitycouncil/sanctions/1988>

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

RISK MANAGEMENT

For Risk Management, the Company will have a risk based approach which includes the following:

- a) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company;
- b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

c) The customers will be monitored on regular basis with built in mechanism for tracking irregular behavior for risk management and suitable timely corrective action.

d) The Company shall prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy. The customer profile shall contain the information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by CredAble. These requirements may be moderated according to the risk perception.

(i) High Risk – (Category A):

High risk customers typically will include:

- a) Individuals and entities listed or identified in – various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267, schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.;
- b) Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
- c) Non - resident Customers (excluding applicants for retail education loans)
- d) High net worth individuals without an occupation track record of more than 3 years
- e) Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (Excluding applicants / beneficial owners who are running affiliated education institutions) – Refer Annexure I
- f) Firms with sleeping partners
- g) Politically exposed persons (PEPs) of Indian/ foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner
- h) Customers with dubious reputation as per public information available or commercially available watch lists.
- i) Gambling/gaming including “Junket Operators” arranging gambling tours;
- j) Jewelers and Bullion Dealers;
- k) Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);
- l) Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;
- m) Customers that may appear to be Multi-level marketing companies etc.
- n) Any borrower/co-borrower working in a country identified as high risk.

(ii) Medium Risk – (Category B):

Medium risk customers typically will include:

- b) Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (i.e. applicants / beneficial owners who are running affiliated education institutions)
- c) Salaried applicant with variable income/ unstructured income receiving Salary in cheque
- d) Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialing (IDD) call service.
- e) Self employed professionals other than HNIs (excluding applicants for retail education loans)
- f) High net worth individuals with occupation track record of more than 3 years
- g) One of more borrowers resident outside India (excluding student going abroad to study)
- h) Companies having close family shareholding or beneficial ownership.
- i) Non face to face to customers (Refer Annexure I)

(iii) Low Risk – (Category C):

Low risk customers typically will include:

- a) Salaried employees with well defined salary structures
- b) People working with government owned companies, regulators and statutory bodies, etc.
- 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
- f) All borrowers resident in India (including student going abroad to study)
- g) 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.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, the Company will obtain senior management approval in such cases to continue the business relationship with such person, and also undertake Enhance due diligence (EDD) measures as specified in Annexure I.

CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification shall be undertaken at the time of commencement of an account-based relationship which would include identify its customers, verify their identity, obtain information on the purpose and intended nature of the business relationship; and determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner.

1. The Company shall undertake identification of customers in the following cases:

-
- a. Commencement of an account-based relationship with the customer;
 - b. Carrying out any international money transfer operations for a person who is not an account holder of the Company.
 - c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;
 - d. Selling their own products, selling third party products as agents and any other product for more than Rs.50,000/-;
 - e. Carrying out transactions for a non-account based customer (walk-in customer), where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
 - f. When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
 - g. The Company shall ensure that introduction is not to be sought while opening accounts.
2. The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.
 3. The Company will obtain Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN.
 4. For the customers that are legal person or entities:
 - i. the Company will verify the legal status for the legal person/ entity through proper and relevant documents;
 - ii. the Company will understand the beneficial ownership and control structure of the customer and determine who the natural persons are and who ultimately controls the legal person.
 5. Additional documentation may be obtained from the customers with higher risk perception as may be deemed fit. This shall be done having regard but not limited to location (registered office address, correspondence address and other addresses as may be applicable), nature of business activity, repayment mode & repayment track record.
 6. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company, at its discretion may at its option, rely on customer due diligence done by a third party, subject to the following conditions:
 - i. Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
 - ii. Necessary information of such customers' due diligence carried out by the third party is immediately obtained by the Company;

- iii. Adequate steps are taken by the Company to satisfy that copies of identification data and other relevant documentation relating to customer due diligence shall be made available from the third party upon request without delay
- iv. 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 the requirements and obligations under the PML Act;
- v. The third party shall not be based in a country/ jurisdiction assessed as high risk;
- vi. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures (as per **Annexure I**), as applicable, will be with the Company.

7. While undertaking customer identification, the Company will ensure that:

- i. Decision-making functions of determining compliance with KYC norms shall not be outsourced.
- ii. The customers shall not be required to furnish an additional OVD, if the OVD submitted for KYC contains proof of identity as well as proof of address e.g. Passport.
- iii. The customers will not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence will be made by the Company. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as cheque books, ATM cards, telephonic conversation, positive address verification, Rent agreement, etc.
- iv. In case of change in the address mentioned on the 'proof of address', fresh proof of address should be obtained within a period of six (6) months.
- v. Enhanced Due diligence measures are indicated in **Annexure I**. An indicative list of the nature and type of documents/information that may be relied upon for customer due diligence / identification is given in **Annexure III**.

In accordance with the above guidelines and guidelines on Customer Due Diligence as detailed in Annexure IV, the Company shall undertake KYC process (Physical- Original Seen & Verified (OSV), live Video – CIP (V-KYC (Video KYC) and Digital - KYC to be carried out by an official of the Company, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent, in the manner detailed in **Annexure II**.

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE:

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

Refer **Annexure-IV** for detailed CDD procedure.

ON-GOING DUE DILIGENCE

The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds. The extent of monitoring shall be aligned with the risk category of the customer. Review of Risk Categorization Indicative list for each category shall be done once in 6 months by Risk Department.

Operations and Sales department will periodically update customer identification data after the account is opened. The periodicity (from the date of account opening/last verification of KYC) of such updation shall be done on annual basis for High, Medium and Low risk category customers which in any case should not exceed two years from the date of account opening/last verification of KYC of all category of customers subjected to following conditions:

- (a) Fresh proofs of identity and address shall not be sought unless:
 - (i) there is a change in the information of the customer as existing in the records of CKYCR; or
 - (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - (iii) the validity period of downloaded documents has lapsed; or
 - (iv) the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

(b) A certified copy of the proof of address forwarded by customers through mail/post, etc., in case of change of address shall be acceptable.

(c) Physical presence of customer at the time of periodic updation shall not be insisted upon. Documents for the purpose of re updation can be accepted through mail/post/courier etc.

(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

(e) Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

BUSINESS PARTNER DUE DILIGENCE PROCEDURE

A BUSINESS PARTNER DUE DILIGENCE (BPDD)

Definition

A Business Partner is defined as "any party who establishes relationships on behalf of their clients with Credable and parties whose employees have access to Credable's data and or systems (outsourcing partners, providers of administrative / IT services, External auditors, data entry

operators, Consultancy firms etc.)” The Outsourcing Policy of Credable governs all Business Partner relationships.

KYC Policy including Risk Categorization will be applicable to all Business Partners including associates / agencies / intermediaries etc.:

- Empaneled Lawyers - Empaneled Valuers - Vendors providing services like Selling Agents, Direct selling team / agents, Collection Agencies, Verification Agencies, Bidders etc. –
- Any other intermediary.

Credable will collect all KYC documents as specified in **Annexures III**.

Due- diligence of Business Partners:

The Business Partner relationships are entered into at the Corporate Office /Regional Office/Head office level. Hence the Heads of Business Units/Departments are responsible to ensure adequate due diligence measures are applied before accepting a Business partner. Following procedure to be followed:

Step 1

Heads of Business Units/Departments should collect information of the following parties as part of the due diligence:

- (i) The Business Partner as a person as such as defined above.
- (ii) Individuals who are authorized to act on behalf of the business partner.
- (iii) The Beneficial Owner (BO) of the business partner.

Step 2

The Heads of Business Units/Departments should screen the names and date of birth/other relevant date of the Business Partner and its BO/Representatives against the freeze /negative lists / Dedup database. In case of hit on the lists screened, enhanced measures should be applied to ascertain the identity of the Business Partner. The enhanced measures are same as the enhanced measures for Customer Acceptance.

Step 3

A pre-employment screening of the staff of the business partners who have /may have access to Company's data or systems should be performed.

Review of Business Partners:

Periodicity

The Business Partner files have to be reviewed with every material change that comes to the notice of Company. Records of business partners should be reviewed every year by Sales and Operations.

Step 1

The Business / Department that has performed the due diligence on accepting the Business Partner is also responsible for periodical review. Audit department shall monitor and ensure all the Business / Department comply with this procedure and perform timely reviews.

Step 2

The review should be performed using the due diligence form for Business Partners. The revised due diligence forms should be kept along with the Agreement.

POLICY ON RISK-BASED APPROACH FOR PERIODIC UPDATION OF KYC DOCUMENTS

CredAble shall periodically update Customer's KYC information / documents after the transaction is entered.

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

Following risk-based approach for periodic updation of KYC has been adopted:

1. Individual Customers:

a) No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the company, customer's mobile number registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter etc.

b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the company, customer's mobile number registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, the Company at its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

c) Accounts of customers, who were minor at the time of opening account, on their becoming major:

In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD

documents as per the current CDD standards are available with the Company. Wherever required, Company may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

d) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 15 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

2. Customers other than individuals:

- a) No change in KYC information:** In case of no change in the KYC information of the legal entity customer, a self-declaration in this regard shall be obtained from the legal entity customer through its email id registered with the company, digital channels (such as online banking / internet banking, mobile application of company), letter from an official authorized by the legal entity in this regard, board resolution etc. Further, company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up to date as possible.
- b) Change in KYC information:** In case of change in KYC information, RE shall undertake the KYC process equivalent to that applicable for on boarding a new legal entity customer.

3. Additional measures:

In addition to the above, company shall ensure that -

- a)** The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the RE has expired at the time of periodic updation of KYC, company shall undertake the KYC process equivalent to that applicable for on boarding a new customer.
- b)** Customer's PAN details, if available with the company, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- c)** An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

- d) In order to ensure customer convenience, company may consider making available the facility of periodic updation of KYC at any branch.
- e) Company shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

MONITORING OF TRANSACTIONS

As per Income Tax Act, 1961, Cash cannot be accepted by any person (Branch / collection staff) over and above Rs. 2,00,000/- (Two Lacs only) for a particular transaction or series of integrally connected transactions. The Company does not accept cash deposits in foreign currency.

As per Income Tax Act, 1961, for any Cash or its equivalent payment over and above Rs. 10,000/-, a 'source of funds' declaration for such cash should be obtained from the Customer/ person depositing / repaying the loan.

Note: Source of funds in cash is through 'sale of immovable property', then Cash or its equivalent for more than Rs. 20,000/- should not be accepted.

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. CredAble 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. CredAble may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve cash over and above Rs. 1 lac should particularly attract the attention of CredAble. Higher risk accounts shall be subjected to intense monitoring.

CredAble 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. AFSL 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 (6) months.

CredAble shall explore the possibility of validating the new account opening applications with various watch lists available in public domain, including RBI watch list.

TRAINING PROGRAMME

CredAble will have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures.

Training requirements will have different focuses for frontline 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.

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 under the supervision of Board 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 audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

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.

RECORD MANAGEMENT

a) Maintenance of records of transactions

The Company shall maintain proper record of the transactions as required under Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) read with Rules 3 of the PML Rules as mentioned below:

- i. All cash transactions of the value of more than Rs. 2 lacs, though by policy the Company does not accept cash deposits in foreign currency.
- ii. All series of cash transactions integrally connected to each other which have been valued below Rs. 2 lacs where such series of transactions have taken place within a month.
- iii. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.
- iv. 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;
- v. records pertaining to identification of the customer and his/her address; and
- vi. All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

An Illustrative List of suspicious transaction pertaining to financial services is given in **Annexure-V**.

b) Records to contain the specified information

The Records referred to above in Rule 3 of PMLA Rules to contain the following information:

- i. the nature of the transactions;
- ii. the amount of the transaction and the currency in which it was denominated;
- iii. the date on which the transaction was conducted; and
- iv. the parties to the transaction.

c) Maintenance and preservation of records:

Section 12 of PMLA requires the Company to maintain records as under:

- i. 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 (5) years from the date of transactions between the clients and CredAble.
- ii. records of the identity of all clients of CredAble is required to be maintained for a period of five years from the date of cessation of transactions between the clients and CredAble.
- iii.
- iv. to make available swiftly, the identification records and transaction data to the competent authorities upon request;

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

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA

In accordance with the requirements under PMLA, the Principal Officer of CredAble will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

- a) Cash Transaction Report (CTR) - If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.
- b) Counterfeit Currency Report (CCR) - All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.
- c) Suspicious Transactions Reporting (STR) - The Company will endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to FIU-IND.

The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed. An indicative list of suspicious transactions is enclosed as **Annexure V**.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts merely on the basis of the STR filed. The employees of CredAble shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

CENTRAL KYC RECORDS REGISTRY (CKYCR)

CKYCR is an entity under CERSAI to receive, store, safeguard and retrieve the KYC records in digital form of a customer. CKYCR manages the KYC for Individual and Legal Entities.

Sharing of information to CKYCR

- Operations to upload KYC record of customer within 10 days of commencement of an account-based relation such as booking of the contract.
- Applicable operational guideline issued by CERSAI for uploading the KYC data shall be followed.
- The KYC of Individual and Legal Entities to be uploaded with CKYCR of the accounts opened on or after 01.04.2017 and 01.04.2021 respectively.
- The KYC Identifier generated by CKYCR to be informed to Individual and Legal Entity as the case may be.
- The CKYCR identifier generated after submission of KYC is required to be communicated to the respective customer.
- Period updation of the KYC information / documents received for Individual and Legal Entities to be done for prior to and after the above-mentioned dates.
- During periodic updation the customers are migrated to current CDD standards (KYC documentation and information).

Use of Information from CKYCR

With an explicit customer consent and submission of KYC Identifier from customer or with the help of acceptable digital solutions, the company shall retrieve the KYC records online/download from CKYCR using KYC Identifier. In such cases customer will not be required to submit KYC / OVD document or information or any other additional identification document or detail, subject to following conditions:

- i. This provision is applicable only for customers falling under Low Risk or Medium Risk category.

- ii. That there is no change in information (such as identification detail, Address, other personal information) of the customer as existed in CKYCR, and
- iii. Address as per application form and CKYC documents is same. Additionally, wherever FI is done, FI should confirm the same address.
- iv. Acceptable vintage of CKYC document used shall be defined by Risk Department from time to time.
- v. The document should be valid at the time of proposed loan and it should be an acceptable KYC document as per the Policy.
- vi. If for any specified reason customer is picked up for additional/enhanced due diligence, then customer Identity and Address shall be verified through appropriate means which may include submission of additional KYC document and personal visit.
- vii. In case contact point verification / customer interaction reports that customer address / KYC detail does not match with the downloaded KYC then fresh KYC shall be obtained.
- viii. Additionally, in case of Non-Individual customers the following documents are required afresh from customer / digital source –
 - Company - Board Resolution, List of Directors, Latest Shareholding pattern, Power of Attorney (if applicable).
 - Partnership Firm - Partnership deed/list of partners with profit sharing ratio, Partnership Authority Letter, Power of Attorney (if applicable).
 - HUF – HUF Letter.
 - AOP/BOI (including Trust, Society etc.) - list of members with beneficial interest percentage Resolution as per entity type, Power of Attorney (if applicable).

GENERAL

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

- (i) Under FATCA and CRS, Credable shall adhere to the provisions of Income Tax Rules 114F, 114G, 114H and determine whether they are a Reporting Financial Institution (RFI) as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:
 - (a) Register on the related e-filing portal of Income Tax Dept. as RFI at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution.
 - (b) Submit online reports using digital signature of the 'Designated Director' by uploading the Form 61B or 'NIL' report, for which, the scheme of Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation – Company will refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules.

- (c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
- (d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- (e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance. The committee shall comprise of Chief Financial Officer (Chairperson), Finance Controller & Chief Compliance Officer as members and shall meet at least annually with a quorum of at least 2 out of 3 members.
- (f) Company shall ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

2. Closure of Accounts/Termination of Financing/Business Relationship:

Where CredAble is unable to apply appropriate KYC measures due to non furnishing of information and/or non-cooperation by the customer, CredAble 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 Chairman & Managing Director or key managerial persons authorized for the purpose.

3. KYC for the Existing Accounts:

While the KYC guidelines 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.

4. Uncovered Provisions: The Company shall adhere to other uncovered provisions given under KYC Master Direction - Know Your Customer (KYC) Direction, 2016 and Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time, which are applicable on the Company.

5. Updation in KYC Policy of Company:

Principal Officer after taking the due approval from the Board of Directors of CredAble shall 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.

Enhanced Due Diligence (EDD) measures

1. Accounts of Politically Exposed Persons (PEPs):

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by 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 have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

1. The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
2. Branch/office shall gather sufficient information on any person/customer/ beneficial owner of this category intending to establish a relationship and check all the information available on the person in the public domain;
3. Branch/office shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a Customer;
4. 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;
5. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
6. 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:

Non-face-to-face onboarding facilitates the company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by company for non- face-to- face customer onboarding..

- a) In case company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. The Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
- c) Apart from obtaining the current address proof, company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

The guidelines for carrying out V-CIP is given at **Annexure II**.

3. Customer's Accounts Opened by Professional Intermediaries:

The Company shall ensure while opening client accounts through professional intermediaries, that:

- (a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (b) Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- (c) Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the RE.
- (d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the Company, the Company shall look for the beneficial owners.
- (e) The Company shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- (f) The ultimate responsibility for knowing the customer lies with the Company.

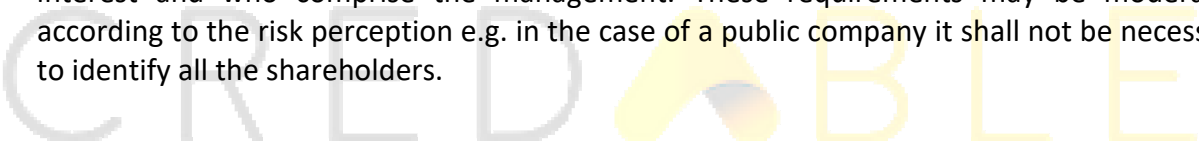
4. Trust/Nominee or Fiduciary Accounts

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 acting, as also obtain details of the nature of the trust or other arrangements in place.

CredAble 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.

5. 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.



ANNEXURE II

Purpose:

KYC verification is conducted to validate the identity of the customer, ensuring compliance with regulatory requirements and mitigating financial risks. Documents such as ID proof, address proof, and any other relevant details are reviewed and verified.

Process Steps:

Step 1- RM/PM to provide consent for fetching both CKYC record of the borrower(s) from CERSAI – Central KYC Registry

Consent is required from -

1. Company (Director)
2. Authorized Signatory (if different than director)
3. Directors/Personal Guarantor
4. Corporate Guarantor (Director)

Step 2 – After the case is approved by the Credit Committee, Pre-D team will send an email to the RM/PM requesting the KYC documentation and consent for the respective individual(s) and company.

Step 3 – Upon receiving the KYC documents and borrowers' consent, Pre-D team will download the KYC from the CERSAI portal and verify the information against the provided documentation.

The following are the three possible scenarios for CKYC:

Sr No	Scenario - 1	Scenario - 2	Scenario - 3
1	CKYC downloaded and KYC documentation Match	CKYC downloaded and KYC documentation does not match	No CKYC
2	No Updation is required	Disbursement Team Should register on CKYC	Disbursement Team Should register on CKYC

Please note – Video KYC /OSV is mandatory for onboarding of any borrower or renewing/ enhancing of any facility.

Step 4 –Below process to be followed for OSV or VKYC. Pre-D team will inform the details to RM/ PM. Basis customers' availability, OSV/ VKYC to be followed.

I.) Original Seen & Verified (OSV): By Business Team RM

1. While on the field visit, RM verify the original documents (*as per Annexure-1*) and obtain a copy of KYC from borrower(s). Also, a photo of individuals to be obtained.
2. Affix OSV details on copy of KYC documents. The details (Stamped or written by RM) are as follows -
 - ✓ Self-certification by writing "Original Seen and Verified" –
 - ✓ RM name & signature
 - ✓ Employee ID
 - ✓ Date (DD:MM: YYYY) & time (HH:MM)
3. Softcopy of the document/s to be submitted by RM by filling up Microsoft form. Link: <https://forms.office.com/r/nwAGm30wmv>
4. Hardcopy of the KYC documents to be submitted before or within 2 working days of first disbursement as per the SPOCs or should be couriered to Lending Operations team.

II) V-KYC: Video KYC of the borrower

1. Pre-D to initiate VKYC verification only once borrower confirms over email that all **original** documents are readily available for VKYC on scheduled time.
2. A VKYC to be called complete only if – (Both for individual and non-individuals)
 - ✓ Aadhar address (mobile no linked with Aadhaar is used to trigger SMS for initiating VKYC) is **matched with the applicant's address** at the time of conducting VKYC.
 - ✓ **Live Face match** with photo on PAN
 - ✓ **Original documents** were shown during the video call.
 - ✓ Authorized signatory / Personal Guarantor **to be available at the registered address** as per Aadhar card at the time of VKYC verification.
 - ✓ Company PAN shown during the video call is verified from GST portal & name from MCA
 - ✓ GST certificate to be shown at the time of Video Call
 - ✓ Unique mobile no to be provided for each individual VKYC
3. Aadhar card need not be verified at the time of VKYC. (Masked Aadhar card)
4. Documentation and checks as per *Annexure-2*:

****For non-Aadhar flow where borrower is unable to start VKYC due to non-verification of Aadhar: Borrower to keep Aadhar handy for verification**

Attachments and References

1. Video KYC demo



VKYC Demo.mp4

2. OSV documentation link where RM has to upload the OSV

<https://forms.office.com/r/nwAGm30wmv>

Points to be noted (Important)

1. All the OSV documents should be Color Print. Xerox copy is not preferable.
2. Written consent from the borrower for downloading CKYC
3. CKYC available on Cersai portal should not be older than one year, in this case KYC will be updated by Credable.
4. V-KYC or OSV needs to be initiated if - Any change / difference in details in the KYC documents provided over email vis-a-vis details as per KYC documents downloaded from CERSAI. – RM must inform us
5. In case OSV confirmation is received on email by RM and physical document is expected to be received later, hence deviation needs to be obtained.

Data will be stored in the below mention format by lending operations

<https://equentia.sharepoint.com/:x:/r/sites/OpsRisk/OpsRisk%20Data/Risk%20Ops%20Data/ISolve/RBI%20CKYC%20data%20-%20Copy.xlsx?d=w780ea73a998a40ea9e1f237bab74bbfc&csf=1&web=1&e=cOaU9i>

Roles of Team Members:

Roles	Responsibilities
Role 1	Pre- D team
Role 2	Disbursement Team

Annexure-1

Constitution	Entity / Company		Authorized signatory / Personal Guarantor (wherever applicable)	
	Proof of Entity	Proof Of Address	Proof of Identity	Proof Of Address
Proprietorship	NA	Any one of the below: - GST certificate / MSME Certificate - Electricity Bill / Phone Bill (previous month)	PAN card	OSV copy of masked Aadhar card
Partnership/LLP	Company Pan card	Any one of the below: - GST certificate / MSME Certificate - Electricity Bill / Phone Bill (previous month)	PAN card	OSV copy of masked Aadhar card
Private limited	Company Pan card	Any one of the below: - GST certificate / MSME certificate - Electricity Bill / Phone Bill (previous month)	PAN card	OSV copy of masked Aadhar card

Annexure-2

Constitution	Entity / Company		Authorized signatory / Personal Guarantor (wherever applicable)		Live Location
	Proof of Entity	Proof of Address	Proof of Identity	Proof of Address	
Proprietorship	NA	GST certificate & Offline verification basis	PAN card	Aadhaar based OTP verification**	Longitude & latitude captured
Partnership/LLP	Company Pan card		PAN card	Aadhaar based OTP verification**	
Private limited	Company Pan card		PAN card	Aadhaar based OTP verification**	

Digital KYC

Digital KYC means the capturing live photo of the customer and OVD/proof of possession of Aadhaar, where offline verification cannot be done, along with latitude and longitude of the location where such live photo is being taken by the company employee. The perquisite norms to execute the facility of Digital KYC:

1. The company required to have Digital Application to execute digital KYC process with customer. The digital KYC process cannot be executed out of company LOS Application system such as Turbo etc.
2. The access of the Application shall be controlled by the company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by company to its authorized official
3. The customer, for the purpose of KYC, shall visit the location of the authorized officer of the company or vice-versa. The original OVD shall be in possession of the customer.
4. The company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further,

the system Application of the company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the custom

5. The Application of the company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color and no other person shall come into the frame while capturing the live photograph of the customer.

6. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and watermarking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

7. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

8. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

9. Once the above-mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the company shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

10. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

11. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

12. The authorized officer of the company shall check and verify that:

(i) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(ii) live photograph of the customer matches with the photo available in the document; and (iii) all of the necessary details in CAF including mandatory field are filled properly;

13. On Successful verification, the CAF shall be digitally signed by authorized officer of the company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

CRED^{ABLE}™

Documents require for initiating Agreement for Private Limited constitution

Sr. NO	Particulars
1	Request you to provide us with the copy of cancelled Cheque of the Company
2	Color Copy of PAN Card of the Company
3	TAN Certificate of the Borrower if TDS/TCS is deducted
4	Kindly confirm us with the name, Phone and Email id for the authorized Signatory.
5	Passport size photograph of the Authorised signatory and personal guarantors. (not more than 3 months letter and on a white background)
6	KYC Documents (Color Copy of PAN and Aadhaar Card) of the authorized Signatory.
7	KYC Documents (Color Copy of PAN and Aadhaar Card) of the Personal Guarantors of the Company.
8	Kindly confirm us with the Phone and Email id of the Personal Guarantor's.
9	Constitutional Documents of the Company i.e (GST certificate ,MSME Certificate , COI, MOA and AOA)
10	Request you to provide us with the end clients contracts/copy of invoices.
11	Request you to provide us with the Email Indemnity (from which we will receive disbursement request) for us to add in agreement
12	Request you to start the process of creation of Common e-mail id and confirm us the credentials to get the same set up.
13	As per the approved CAN request you to start the process for creation of virtual account.
14	Kindly provide the Transaction Fee details which the Borrower will pay towards every drawdown request.

Documents require for initiating Agreement for Proprietor constitution

Sr. NO	Particulars
1	Request you to provide us with the copy of cancelled Cheque of proprietorship firm
2	KYC Documents (Color Copy of PAN and Aadhaar Card) of Proprietor
3	Passport size photograph of the Authorised signatory and personal guarantors. (not more than 3 months letter and on a white background)
4	Constitutional Documents of the Company i.e (GST certificate and MSME Certificate) of Proprietorship Firm
5	Request you to provide us with the end clients contracts/copy of invoice of End clients if any.
6	Request you to provide us with the Email Indemnity (from which we will receive disbursement request) for us to add in agreement
7	Cancel Cheque or Bank statement of the Proprietorship firm
8	Request you to start the process of creation of Common e-mail id and confirm us the credentials to get the same set up.
9	As per the approved CAN request you to start the process for creation of virtual account.
10	Kindly provide the Transaction Fee details which the Borrower will pay towards every drawdown request

Documents require for initiating Agreement for Partnership constitution

Sr. NO	Particulars
1	Request you to provide us with the copy of cancelled Cheque of the Partnership Firm.
2	Request you to provide us with the color copy of PAN Card of Partnership Firm.
3	Kindly confirm us with the name, Phone and Email id for the authorized Signatory.
4	Passport size photograph of the Authorised signatory and personal guarantors. (not more than 3 months letter and on a white background)
5	KYC Documents (color copy of PAN and Aadhaar Card) of the Personal Guarantors of the Partnership Firm.
6	Kindly confirm us with the Phone and Email id of the Personal Guarantors.
7	KYC Documents (color copy of PAN and Aadhaar Card) of the authorized Signatory.
8	Request you to provide us with the Partnership Deed, GST, MSME Certificate of the Partnership Firm.
9	Request you to provide us with the end clients contacts of all the end clients.
10	Request you to provide us with the Email Indemnity (from which we will receive disbursement request) for us to add in the FA.
11	Request you to start the process of creation of Common e-mail id and confirm us the credentials to get the same set up.
12	Kindly provide the Transaction Fee details which the Borrower will pay towards every drawdown request.
13	As per the approved CAN request you to start the process for creation of virtual e-mail.
14	Please provide TAN and it's supporting documents for the mentioned vendors. If supporting document is not available, then kindly provide snapshot from Income Tax portal.

Documents require for initiating Agreement for LLP constitution

Sr. NO	Particulars
1	Request you to provide us with the copy of cancelled Cheque of LLP Firm
2	Color Copy of PAN Card of the LLP Firm .
3	TAN Certificate of the Borrower if TDS/TCS is deducted
4	Passport size photograph of the Authorised signatory and personal guarantors. (not more than 3 months letter and on a white background)
5	Kindly confirm us with the name, Phone and Email id for the authorized Signatory.
6	KYC Documents (Color Copy of PAN and Aadhaar Card) of the authorized Signatory.
7	KYC Documents (Color Copy of PAN and Aadhaar Card) of the Personal Guarantors of the LLP Firm.
8	Kindly confirm us with the Phone and Email id of the Personal Guarantors
9	Constitutional Documents of the Company i.e (GST certificate ,MSME Certificate , LLP Deed)
10	Request you to provide us with the end clients contracts/copy of invoices.
11	Request you to provide us with the Email Indemnity (from which we will receive disbursement request) for us to add in agreement
12	Request you to start the process of creation of Common e-mail id and confirm us the credentials to get the same set up.
13	As per the approved CAN request you to start the process for creation of virtual account.
14	Kindly provide the Transaction Fee details which the Borrower will pay towards every drawdown request.

ANNEXURE – IV

Customer Due Diligence (CDD) Procedure in case of Individuals

(i) While undertaking CDD, following information will be obtained from an individual while establishing an account-based relationship with an 'Individual' or dealing with the individual who is a Beneficial Owner, Authorised Signatory or the Power of Attorney Holder related to any legal entity:

a) The Aadhaar Number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act 2016 (18 of 2016); or

(ii) The customer 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; or

(ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

(ii) PAN or equivalent e-document thereof or Form No. 60 as defined in Income-Tax Rules, 1962, and

(iii) 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 here the customer has submitted:

- Aadhaar number under clause (a), notified under first proviso to sub-section (1) of section 11A of the PML Act, BHFL 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, self declaration to that effect must be obtained from the customer.
- The proof of possession of Aadhaar number under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.
- 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 Digital KYC Process as given in **Annexure II**.
- 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 by the rules and regulations reproduced under **Annexure II**.

- KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with in accordance with CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) as detailed under.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Company 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.

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 infirmity on 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. CDD done in this manner shall invariably be carried out by an official of the RE and such exception handling shall also be a part of the concurrent audit as mandated in paragraph 8. REs shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the RE and shall be available for supervisory review.

Explanation 1: The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such **customer redacts or blacks out only the first eight digit of** Aadhaar Number (on copy of Aadhaar Letter/ Aadhaar Card obtained) through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

(v) List of Officially Valid Documents:

- a) Passport,
- b) Driving License,
- c) Voter's Identity Card issued by Election Commission of India,
- d) Proof of possession of Aadhaar Number*, i.e. Aadhaar letter, Aadhaar Letter downloaded

from UIDAI website (e-Aadhaar), Aadhaar Card, Aadhaar Secure QR Code, Aadhaar Paperless Offline e-KYC (an XML document generated by the UIDAI),*(Ensure to redact/ blacken only the First Eight Digits of Aadhaar No. (on copy of Aadhaar Letter/ Aadhaar Card obtained)

e) Job Card issued by NREGA duly signed by an officer of the State Government,

f) Letter issued by the National Population Register containing details of Name, Address of the customer having photograph of the card holder.

(vi) In case the OVD furnished by the customer does not contain updated address, the following documents or the equivalent e-documents thereof shall be Deemed to be OVDs (DOVD) for the limited purpose of Proof of Address: -

a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill),

b) Property or Municipal tax receipt,

c) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public-Sector Undertakings, if they contain the address,

d) Letter 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 license agreements with such employers allotting official accommodation.

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.

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

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

(vii) A customer already having an account-based relationship with the Company, shall submit his Permanent Account Number or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily ceased to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, Company shall give the customer an accessible notice and a reasonable opportunity to be heard.

Explanation: - For the purpose of this clause, "temporary ceasing of operations" in relation an account means the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this clause;

In case of asset accounts, such as **loan accounts**, for the purpose of ceasing the operation in the account, only **credits shall be allowed**.

(viii) If a customer having an existing account-based relationship with the Company gives in writing to the company that he/ she does not want to submit his/her PAN or Form No. 60, as the case may be, the customer's account with the company shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer. The Company shall duly inform the customer about this provision while opening the account.

(ix) List of the nature and type of documents/ information that may be relied upon for customer identification pertaining to Individuals, Sole Proprietary Firms, Legal Entities-Company, Partnership Firm, Trust, Unincorporated Association/Body of Individuals, Juridical Persons, BO is given in the **Annexure III**.

(x) Accounts Opened using OTP based e-KYC, in non-face-to-face mode:

Accounts opened using Aadhaar 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. As a risk-mitigating measure for such accounts, the Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. REs shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- v. 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 (vi) below is complete.
- vi. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- vii. 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.
- viii. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per paragraph 16 or as per paragraph 18

(V-CIP) is carried out. If Aadhaar details are used under paragraph 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

- ix. 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.
- x. 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 with any other RE. Further, while uploading KYC information to CKYCR, Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other Company's shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- xi. 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.

(xi) Video Customer Identification Process (V-CIP)

The Company 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.

Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in CDD Measures for Sole Proprietary firms detailed below, apart from undertaking CDD of the proprietor.

- ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per paragraph (x) given above.

- iii) Updation/ Periodic updation of KYC for eligible customers

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

(a) V-CIP Infrastructure

- i) The Company 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. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE only and all the data including

video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

ii) The Company 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 Company.

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 the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservice 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

i) The 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 RE

specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.

iii) 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.

iv) Any prompting observed at end of customer shall lead to rejection of the account opening process.

v) 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.

vi) The authorised official of the RE 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:

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR), using the KYC identifier provided by the customer

d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker

The Company shall ensure to redact or blackout the Aadhaar number in terms of aforesaid provisions.

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 three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, REs shall ensure that the video process of the V-CIP is undertaken within three working 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.

vii) 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.

viii) 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.

ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

x) The authorised official of the RE 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.

xi) Assisted V-CIP shall be permissible when banks take help of Business 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.

xii) 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.

xiii) 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 Company.

The V-CIP process is covered in **Anenxure II**.

(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. The Company 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 said Master directions, 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.

The format under which the Company maintain such data is covered in **Anenxure II**.

CDD Measures for Identification of Beneficial Owner (BO):

For opening an account of a Legal Person who is not a natural person, the Beneficial Owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the PMLA Rules to verify his/her identity shall be undertaken keeping in view the following:

(i) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

(ii) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Beneficial Owner Declaration format is given at **Annexure VI**.

CREDABLE™

ANNEXURE - V

A. Broad categories of reason for suspicion and examples of suspicious transactions are indicated as under:**Identity of client**

- False identification documents
- Identification documents which could not be verified within reasonable time
- Accounts opened with names very close to other established business entities

Background of client

- Suspicious background or links with known criminals

Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale

Activity in accounts

- Unusual activity compared with past transactions

Nature of transactions

- Unusual or unjustified complexity
- Involves proceeds of a criminal / illegal activity, regardless of the value involved
- No economic rationale or bonafide purpose
- Frequent purchases of drafts or other negotiable instruments with cash
- Nature of transactions inconsistent with what would be expected from declared business
- Reasonable ground of suspicion that it may involve financing of activities relating to terrorism and/or account holder / beneficial owner linked or related to terrorist, terrorist organization or those who finance or attempt to finance terrorist activities.

Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client's apparent financial standing

B. Illustrative list of Suspicious Transactions

- Reluctant to part with information, data and documents
- Submission of false documents, purpose of loan and detail of accounts
- Reluctance to furnish details of source of funds of initial contribution
- Reluctance to meet in person, representing through power of attorney
- Approaching a distant branch away from own address
- Maintaining multiple accounts without explanation

- Payment of initial contribution through unrelated third party account
- Suggesting dubious means for sanction of loan
- Where transactions do not make economic sense
- Where doubt about beneficial ownership
- Encashment of loan through a fictitious bank account
- Sale consideration quoted higher or lower than prevailing area prices
- Request for payment in favor of third party with no relation to transaction
- Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent
- Frequent request for change of address
- Overpayment of installments with a request to refund the overpaid amount
- Approvals/sanctions from authorities are proved to be fake
- Overpayment of installments with a request to refund the overpaid amount

ANNEXURE VI

Beneficial Ownership Declaration



VERSION HISTORY

Version	Date	Change
1.1	June 24, 2019	Policy approved
1.2	November 29, 2019	Annual review of the Policy
1.3	June 23, 2020	Reviewed
1.4	February 20, 2025	Reviewed, amended and approved
1.5	August 19th, 2025	Reviewed, amended and approved