

InCred Capital Financial Services Private Limited
Know Your Customer & Anti-Money Laundering Policy

1. SCOPE

1.1 Applicability This “Know Your Customer and Anti-Money Laundering Policy” (the Policy) will apply to InCred Capital Financial Services Private Limited throughout the website and Credits Private Limited (“the Company”), its employees and its agents/ representatives. This Policy will require the Company’s employees and its agents/ representatives to: • Protect the Company from being used for any type of money laundering or terrorist funding activities; • Comply with the applicable Anti-Money Laundering (AML) Laws and the Company’s KYC & AML Policy & Procedures in letter and spirit; • Be alert and escalate suspicious activity and not knowingly provide advice or other assistance to individuals who attempt to violate Anti Money Laundering Laws or this Policy. Knowledge includes the concept of ‘willful blindness’ (failure to make appropriate inquiries when faced with suspicion of wrongdoing) and ‘conscious avoidance of knowledge’; • Conduct themselves in accordance with the highest ethical standards; and • Co-operate with the regulatory authorities and the Financial Intelligence Unit as per the applicable laws.

1.2 Effective Date This Policy shall be effective from the date of approval of this policy

1.3 Review of Policy The Policy shall be reviewed as and when required by the applicable rules and regulations.

1.4 Implementation & Monitoring of Policy The Risk Management Committee (RMC) will monitor and supervise implementation of the Policy.

1.5 Policy Approval The Policy and any significant changes therein shall be approved by the Board of Directors or The Risk Management Committee of the Company.

2. BACKGROUND

The term ‘Money Laundering’ refers to act of concealing or disguising origin and ownership of proceeds from criminal activities 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 & investment products, financing of equipment or other property that could be used to facilitate terrorism and other criminal activity. Almost every crime with a profit motive can create proceeds that can be laundered. For example, fraud, theft, illegal drug sales, organized crime, bribery, corruption of government officials and human trafficking can create illegal funds that a criminal seeks to convert into legitimate property without raising suspicion. Tax evasion and violations of fiscal laws can also lead to money laundering. Generally, the process of Money Laundering involves three stages, viz.

- (i) Placement;
- (ii) Layering; and
- (iii) Integration.

As illegal funds move from the placement stage to the integration stage, it becomes increasingly harder to detect and trace back to the illegal source.

- Placement is the point where illegal funds first enter the financial system. The deposit of illegal cash into an account or the purchase of money orders, cashier’s checks or other financial product is made. Non-bank financial institutions, such as currency exchanges, money remitters, casinos, and check-cashing services can also be used for placement.

- 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.

- 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. A financial institution or other business may be used at any point in the process of money laundering. The criminals and other anti-social elements keep coming-up with innovative means to launder money and no financial institution or business is immune from possible victimization. To address issue of money laundering, the Government of India and other countries around the world have made money laundering a crime and prescribed regulatory requirements for compliance by the banks, financial companies/ institutions and other regulated/ reporting entities to prevent and detect money laundering. To prevent money-laundering in India and to provide for confiscation of property derived from or involved in money-laundering and related matters, the Government of India enacted the Prevention of Money Laundering Act, 2002 (PMLA), as amended from time to time. Further, the

PMLA and necessary Notifications/ Rules thereunder have been published and amended thereafter. As per the Prevention of Money Laundering Act 2002, "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. Further, "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 and the Rules notified thereunder impose obligation on banking companies, financial institutions (which includes chit fund company, a co-operative bank, a non-banking financial company and a housing finance institution) and other defined intermediaries to verify identity of clients, maintain records and furnish requisite information to Financial Intelligence Unit- India (FIU-IND). 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) has prescribed the Reserve Bank of India {Know Your Customer (KYC)} Directions, 2016 ("RBI KYC Directions") in order to ensure compliance by every entity regulated by RBI ("Regulated Entity") with the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.. In accordance with the RBI KYC Directions, the Company is required to have a Know Your Customer (KYC) Policy duly approved by its Board of Directors or any committee of the Board to which power may be delegated. The KYC and AML Policy has been prepared considering the following key elements: a) To lay down the criteria for Customer Acceptance (CAP); b) Risk Management; c) To lay down criteria for Customer Identification Procedures (CIP); d) To establish procedures for monitoring of transactions as may be applicable;

3. DEFINITIONS For this Policy, definition of various terms used is as under:

3.1 Beneficial Owner (BO)

a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means. Explanation- For the purpose of this sub-clause-

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

ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals. Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official. d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3.2 Cash Transaction Report (CTR)- CTR will include the following:

a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency.

3.3 Central KYC Records Registry (CKYCR) means an entity defined under Rule 2(1)(aa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

3.4 Counterfeit Currency Transaction- All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine. These cash transactions should also include transactions where forgery of valuable security or documents has taken place.

3.5 Customer- For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.6 Customer Due Diligence (CDD)- Identifying and verifying the customer and the beneficial owner using

'Officially Valid Documents' as a 'Proof of Identity' and a 'Proof of Address'.

3.7 Designated Director- means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the Rules thereunder and includes:-

- a) the Managing Director or a whole-time Director duly authorized by the Board of Directors,
- b) A person of senior management official designated by the Company as "Designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012. However, in no case, the Principal Officer should be nominated as the "Designated Director".

3.8 KYC Templates means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities, as required by the relevant Rules.

3.9 Non-face-to-face customers- Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials.

3.10 Officially valid document (OVD)- Any document notified/ advised by the Central Government/ Regulatory Authorities as officially valid document for verifying identity and proof of address of customers. As on date, OVD means the passport, the Driving License, the Permanent Account Number (PAN) Card, 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, Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. Explanation: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address. Further, 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.

3.11 On-going Due Diligence- Regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

3.12 Periodic Updation means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI, the PMLA and the Rules thereunder.

3.13 Politically Exposed Persons- Individuals who are or have been entrusted with prominent public functions, e.g., Heads of States/Governments, senior politicians, senior government/ judicial/military officers, senior executives of state-owned corporations, important political party officials etc.

3.14 Principal Officer (PO)- An official designated by the Board of Directors of the Company for overseeing and managing the KYC & AML policies and processes. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

3.15 'Senior Management' for the purpose of KYC compliance shall include members of the Executive Committee, Designated Director, Principal Officer (PO) and his supervisor.

3.16 Simplified procedure- means the procedure for undertaking customer due diligence in respect of individual customers, who desires to open an account is not able to produce documents as per CDD procedures of the policy, the Company may at its discretion open account subject to the following conditions:

- a. The Customer shall submit a self-attested photograph.
- b. The designated officer of the Company shall certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
- c. The account shall remain operational initially for a period of twelve months, within which the customer has to furnish identification information.
- d. The identification process is to be completed for all the existing accounts opened on the basis of introduction earlier, within a period of six months.
- e. balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time
- f. the total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
- g. The customer shall not be permitted to undertake further transactions until the full KYC procedure is completed in case Directions (e) and (f) above are breached by him.
- h. The Customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (e) and (f) above.

3.17 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 the proceeds of crime, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to have no economic rationale or bona fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

3.18 Transaction- 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) establishing or creating a legal person or legal arrangement.

3.19 Walk-in Customer- means a person who does not have an account based relationship with the Company, but undertakes transactions with the Company. 1. CUSTOMER ACCEPTANCE POLICY (CAP) In line with the RBI Directions, the PMLA and the Rules thereunder, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers. The features of the CAP are detailed below:

- a) The Company will not open any account(s) in anonymous, fictitious or 'benami' name(s).
- b) No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.
- c) No transaction or account based relationship will 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 will be specified
- e) Optional or additional information will be obtained with an explicit consent of the customer after the account is opened.
- f) CDD Procedure will be followed for all the joint account holders, while opening a joint account. However, if an existing KYC compliant customer desires to open another account, there shall be no need for a fresh CDD exercise
- g) Circumstances in which, a customer is permitted to act on behalf of another person/entity, will be clearly spelt out.
- h) The Company will ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. For this purpose, the Company shall maintain lists of individuals or entities issued by RBI, United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious and reported.
- i) Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company will conduct appropriate due diligence. The nature and extent of basic due diligence measures to be conducted at the time of establishment of account opening/ relationship, would depend upon the risk category of the customers and involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the risks posed by the applicant and the applicant's expected use of the Company's products and services from an AML perspective.
- j) The Company may rely on third party verification subject to the conditions prescribed by the RBI, the PMLA and the Rules thereunder in this regard.
- k) For non-face-to-face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such customers.
- l) Relationship/ opening of accounts shall be established and the beneficiary of the relationship/ account shall also be identified.
- m) The information collected from the customer shall be kept confidential.
- n) Appropriate Enhanced Due Diligence (EDD) measures shall be adopted for high risk customers from AML

perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs) and their family members/close relatives.

o) In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall be adopted.

p) Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision. The aspects mentioned in the CAP would be reckoned while evolving the KYC/AML procedures for various types of customers and products. However, while developing the KYC/CDD procedures, the Company will ensure that its procedures do not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society.

2. RISK MANAGEMENT

5.1 For Risk Management, the Company shall 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 RE;

b) Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location 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.

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.

5.2 High and Medium Risk from AML perspective- A customer that is likely to pose a higher than average risk may be categorized high or medium risk depending on background, nature & location of customer, his/ her profile, scale of customer's volume, his/ her financials and social status etc. Due diligence measures will be applied based on the risk assessment. The Company shall apply enhanced due diligence measures for higher risk customers, especially those for whom the sources of funds are not clear.

a) Indicative list of High Risk Customers

i) Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;

ii) Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;

iii) Individuals and entities in watch lists issued by Interpol and other similar international organizations;

iv) Customers with dubious reputation as per public information available or commercially available watch lists;

v) Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;

vi) 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.;

vii) Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;

viii) Non-face-to-face customers;

ix) High net worth individuals;

x) Firms with 'sleeping partners';

xi) Companies having close family shareholding or beneficial ownership;

xii) Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;

xiii) Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low level staff does not constitute physical presence;

xiv) Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed;

xv) Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.;

xvi) Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;

xvii) Gambling/gaming including "Junket Operators" arranging gambling tours;

xviii) Jewelers and Bullion Dealers;

xix) 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);

xx) Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries);

- xxi) Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
- xxii) Customers that may appear to be Multi-level marketing companies etc.

b) Indicative list of Medium Risk Customers

- i) Stock brokerage;
- ii) Import / Export;
- iii) Gas Station;
- iv) Car / Boat / Plane Dealership;
- v) Electronics (wholesale);
- vi) Travel agency;
- vii) Telemarketers;
- viii) Providers of telecommunications service, internet café, International direct dialing (IDD) call service.

5.3 Low Risk from AML perspective- All other customers (other than High and Medium Risk category) whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

6. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

a) The Company will undertake identification of customers in the following cases:

- i) Commencement of an account-based relationship with the customer;
- ii) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;
- iii) Selling their own products, selling third party products as agents and any other product as applicable;
- iv) Carrying out transactions for a non-account based customer (walk-in customer).

b) 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.

c) The Company will obtain and verify 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.

d) 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 are the natural persons who ultimately control the legal person.

e) 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, profile, source of income etc.

f) An indicative list of the nature and type of documents/ information that may be relied upon for customer identification is provided in the 'Annexure A' of this Policy. The documents to be accepted by the Company for customer identification will be based on the regulatory prescriptions from time to time and may be implemented/ revised after approval from the Principal Officer and the Head of Risk/ Credit function.

g) For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may 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 within two days from the third party or from the Central KYC Records Registry;
- ii) 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
- iii) 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;
- iv) The third party shall not be based in a country/ jurisdiction assessed as high risk;
- v) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.
- h) 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.
 - 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 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 months.

7. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

7.1 CDD Procedure in case of Individuals

a) The Company will obtain the following documents from an individual while establishing an account based relationship:

i) one certified copy of an OVD as defined above containing details of identity and address;

ii) one recent photograph; and

iii) such other documents pertaining to the nature of business or financial status specified by the Company. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer

b) The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification and the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process will be treated as an 'Officially Valid Document'. However, before commencing the e-KYC process, there should be explicit consent and authorization from the individual customer authorizing UIDAI to release his/ her identity/address through biometric authentication to the Company or its Business Correspondents (BCs). Further, the Company may also opt for One Time Pin (OTP) based e-KYC process for on-boarding of customers subject to the following conditions:

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

ii. the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete. iii. the aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.

iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

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

vi. REs 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.

c) The Company may print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal, if such a customer knows only his/her Aadhaar number or if the customer carries only a copy of Aadhaar downloaded from a place/source elsewhere, provided, the prospective customer is physically present in the branch of the Company.

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

e) If a person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative as provided at sub-section 77 of Section 2 of the Companies Act, 2013, read with Rule 4 of Companies (Specification of definitions details) Rules, 2014, with whom the person is staying, as the 'proof of address'; Explanation: A declaration from the relative that the said person is a relative and is staying with him/her shall be obtained

f) If a customer categorised as 'low risk' expresses inability to complete the documentation requirements on account of any genuine reason, and where it is essential not to interrupt the normal conduct of business, the Company may, at its discretion, complete the verification of identity of the customer within a period of 6 months from the date of establishment of the relationship.

g) In respect of customers who are categorised as 'low risk' and are not able to produce any of the OVDs mentioned, 'simplified procedure' may be applied, Explanation: During the periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorised as 'moderate or "high' risk category, then the Company shall obtain one of the six standard OVDs listed at para 3.10 above for proof of identity and proof of address immediately.

h) KYC verification once done by one branch/office of the Company shall be valid for transfer of the account to any other branch/office of it, provided full KYC verification has already been done for the concerned account and

the same is not due for periodic updation and a self-declaration from the account holder about his/her current address is obtained in such cases.

7.2 CDD Measures for Sole Proprietary firms

a) For opening an account in the name of a sole proprietary firm, a certified copy of an OVD as mentioned above, containing details of identity and address of the individual (proprietor) shall be obtained.

b) In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

- i) Registration certificate;
- ii) Certificate/ License issued by the municipal authorities under Shop and Establishment Act;
- iii) Sales and income tax returns;
- iv) CST/VAT/GST certificate;
- v) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities;
- vi) License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute;
- vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities;
- viii) Utility bills such as electricity, water, and landline telephone bills. In cases where the Company is satisfied that it is not possible to furnish two such documents, it may accept only one of those documents as proof of business/ activity, subject to contact point verification and collection of such other information and clarification as would be required to establish the existence of such firm. Further, it should be satisfied that the business activity has been verified from the address of the proprietary concern.

7.3 CDD Measures for Legal Entities

a) For opening an account of a company, one certified copy of each of the following documents shall be obtained:

- i) Certificate of incorporation.
- ii) Memorandum and Articles of Association.
- iii) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
- iv) Officially valid documents in respect of managers, officers or employees holding an attorney to transact on its behalf.

b) For opening an account of a partnership firm, one certified copy of each of the following documents shall be obtained:

- i) Registration certificate.
 - ii) Partnership deed.
 - iii) Officially valid documents in respect of the person holding an attorney to transact on its behalf.
- c) For opening an account of a trust, one certified copy of each of the following documents shall be obtained:
- i) Registration certificate.
 - ii) Trust deed.
 - iii) Officially valid documents in respect of the person holding a power of attorney to transact on its behalf.

d) For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the following documents shall be obtained:

- i) Resolution of the managing body of such association or body of individuals;
- ii) Power of attorney granted to transact on its behalf;
- iii) Officially valid documents in respect of the person holding an attorney to transact on its behalf; and
- iv) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals. Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.

e) For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents shall be obtained:

- i) Document showing name of the person authorised to act on behalf of the entity;
- ii) Aadhaar/ PAN/ Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf ; and
- iii) Such documents as may be required by the Company to establish the legal existence of such an entity/ juridical person.

7.4 Selling Third party products- The Company, if acting as agents while selling third party products as per regulations in force from time to time, will comply with the following aspects:

- i. The identity and address of the walk-in customer shall be verified for the transactions above rupees fifty thousand;
- ii. Transaction details of sale of third-party products and related records shall be maintained.

- iii. Monitoring of transactions for any suspicious activity will be done.
- iv. transactions involving rupees fifty thousand and above shall be undertaken only by:
 - a) debit to customers' account or against cheques; and
 - b) obtaining and verifying the PAN given by the account based as well as walk-in customers.

7.5 Enhanced Due Diligence

- a) Accounts of non-face-to-face customers: The Company will include additional procedures i.e., certification of all the documents presented, calling for additional documents and the first payment to be effected through the customer's KYC-complied account with another regulated entity for enhanced due diligence of non-face to face customers.
- b) Accounts of Politically Exposed Persons (PEPs): The Company will have the option of establishing a relationship with PEPs, provided that:
 - i) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
 - ii) the identity of the person shall have been verified before accepting the PEP as a customer;
 - iii) the decision to open an account for a PEP is taken at a senior level in accordance with the Company's Customer Acceptance Policy;
 - iv) all such accounts are subjected to enhanced monitoring on an on-going basis;
 - v) 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; vi) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable. The above will also be applicable to accounts where a PEP is the beneficial owner.
- c) Client accounts opened by professional intermediaries: REs 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. REs 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. REs shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.
 - d. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of 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 Company, the Company shall look for the beneficial owners.
 - e. REs 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.

7.6 Simplified Due Diligence

- a) For Self Help Groups (SHGs)
 - i) KYC verification of all the members of SHG as per the CDD procedure mentioned in the Policy shall not be required while opening the savings bank account of the SHG.
 - ii) KYC verification as per the CDD procedure mentioned in the Policy of all the office bearers shall suffice.
 - iii) No separate KYC verification as per the CDD procedure mentioned in the Policy of the members or office bearers shall be necessary at the time of credit linking of SHGs

7.7 Identification of Beneficial Owner 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 to verify his/her identity shall be undertaken keeping in view the following:

- a) 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.
- b) 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.

8. MONITORING OF TRANSACTIONS/ ON-GOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC procedures. The Company shall 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 Company shall identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the

account. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

8.1 The Company will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. The Company will carry such review of risk categorization of customers at a periodicity of not less than once in six months.

8.2 Periodic Updation- The Company will conduct periodic updation of KYC documents 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 subject to the following conditions:

a) Fresh proofs of identity and address shall not be sought at the time of periodic updation from customers who are categorised as 'low risk', when there is no change in status with respect to their identities and addresses and a self-certification to that effect is obtained.

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

c) Physical presence of low risk customer at the time of periodic updation shall not be insisted upon.

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.

f) E-KYC process using OTP based authentication for periodic updation is allowed provided while onboarding, the customer was subjected to proper KYC process.

9. REPORTING TO FINANCIAL INTELLIGENCE UNIT- INDIA

9.1 In accordance with the requirements under PMLA, the Company 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.

9.2 Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports- The Company will maintain utmost confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the FIU-IND/ higher authorities. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

10. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company will capture the KYC information for sharing with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, under the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company will upload the KYC data pertaining to all types of prescribed accounts with CKYCR, as and when required, in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

11. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

If applicable to the Company, it will adhere to the provisions of Income Tax Rules 114F, 114G and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take the following requisite steps for complying with the reporting requirements:

i. Register on the related e-filing portal of Income Tax Department as a Reporting Financial Institution;

ii. Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to;

iii. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H;

- iv. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.;
- v. Constitute a “High Level Monitoring Committee” under the Designated Director or any other equivalent functionary to ensure compliance;
- vi. 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.

12. INDEPENDENT EVALUATION

To provide reasonable assurance that its KYC and AML procedures are functioning effectively, an audit of its KYC and AML processes will be covered under Internal Audit of the Company. 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.

13. RESPONSIBILITIES OF THE SENIOR MANAGEMENT

13.1 Designated Director- The Company shall nominate a “Designated Director” to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder. The “Designated Director” can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the “Designated Director”.

13.2 Principal Officer- An official (having knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business) shall be designated as the Principal Officer of the Company. The Principal Officer will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

13.3 Key Responsibilities of the senior management

- i) Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under PMLA.
- ii) Proper implementation of the company's KYC & AML policy and procedures.

14. RECORD MANAGEMENT

14.1 Record-keeping requirements- The Company shall introduce a system of maintaining proper record of transactions required under PMLA as mentioned below:

- a) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;
- b) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign;
- c) 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 or a document has taken place facilitating the transactions;
- d) all suspicious transactions whether or not made in cash; and
- e) records pertaining to identification of the customer and his/her address; and
- f) should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

14.2 Records to contain the specified information- The records should contain the following information:

- a) the nature of the transactions;
- b) the amount of the transaction and the currency in which it was denominated;
- c) the date on which the transaction was conducted; and
- d) the parties to the transaction.

14.3 Maintenance and Preservation of records

- a) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions referred in para 14.1 above;
- b) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity;
- c) records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card etc.) obtained while opening the account and during the course of business relationship would continue to be preserved for at least 5 years after the business relationship is ended;
- d) records may be maintained either in hard or soft format.

15. HIRING OF EMPLOYEES, THEIR TRAINING AND EDUCATION OF CUSTOMERS

15.1 Hiring of Employees and Employee training- Adequate screening mechanism as an integral part of their

personnel recruitment/hiring process shall be put in place. On-going employee training programme will be put in place so that the members of staff are adequately trained in KYC & AML policy.

15.2 Implementation of KYC Procedures requires the Company to seek information which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. To meet such situation, it is necessary that the customers are educated and apprised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company. To educate the customers, the Company will arrange FAQs on KYC and AML measures. Such FAQs may be made available to the customers directly, on request, or through the Company's website.