POLICY ON
KNOW YOUR CUSTOMER
&
ANTI MONEY LAUNDERING
NEUZEN FINANCE PRIVATE LIMITED
(FORMERLY KNOWN AS UMANG TRADING PVT.LTD.)

CONTENTS

Know Your Customer Guidelines and Anti-Money Laundering Standards

The Reserve Bank of India (RBI) has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board. The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently.

The main objective of this policy is to enable the Company to have positive identification of its customers. Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company. This policy is applicable to all categories of products and services offered by the Company.

1. PREAMBLE

a. Board of Directors (the "Board") of **Neuzen Finance Private Limited** (formerly known as Umang Trading Pvt. Ltd.)(The "**Company**" or "**NFPL**"), has adopted the following policy regarding salient features of Know Your Customer ('**KYC**') and Anti-Money Laundering ("**AML**") norms for **Neuzen Finance Private Limited** as prescribed by Reserve Bank of India ("**RBI**").

2. Purpose (Objectives)

a. The policy has been framed in accordance with RBI (Know Your Customer (KYC) Directions, 2016. Further, the policy has been amended in accordance with the changes carried out in the PML Rules and thereafter and is subject to the final judgment of the Hon'ble Supreme Court in the case of Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India(Aadhaar case).

b. As per the above-referred master circular, NFPL is required to adopt the guidelines contained therein with suitable modifications in accordance with the Company's business activity and ensure that a proper policy framework on KYC and AML measures are formulated and put in place with the approval of the Board.

c. Further, the policy is amended in accordance with the changes carried out in the RBI (Know Your Customer (KYC) Directions, 2016.

d. This policy document envisages the establishment and adoption of measures and procedures relating to KYC and AML for NFPL in accordance with the requirements prescribed by RBI and modified from time to time.

e. The main objective of this policy is to prevent the Company from being used intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The following four key elements form a part of the policy:

i. Customer Acceptance Policy
ii. Customer Identification Procedures
iii. Risk Management
iv. Monitoring of Transactions

3. Definitions

a. "Accounts" shall mean all the loan accounts of the respective customers of the company.

b. "Beneficial Owner" is a natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercise ultimate effective control over a judicial person.

c. "Customer" means a person who is engaged in a financial transaction or activity with a NFPL and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

d. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

e. "Customer identification" means undertaking the process of CDD.

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

In case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

i. authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
ii. branches of overseas banks with whom Indian banks have relationships,
iii. Notary Public abroad,
iv. Court Magistrate,
v. Judge,
vi. Indian Embassy/Consulate General in the country where the non-resident customer resides.

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

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

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

j. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

k. "Officially Valid Document" (OVD) means

i. the passport,
ii. the driving licence,
iii. Proof of possession of Aadhaar number,
iv. the Voter's Identity Card issued by the Election Commission of India,
v. Job card issued by NREGA duly signed by an officer of the State Government and
vi. Letter issued by the National Population Register containing details of name and address.
vii. 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.
viii. 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: -

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; Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; the customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

ix. 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.

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.

l. "Person" has the same meaning assigned in the Section 2(s) of the Prevention of Money Laundering Act and includes:

i. an individual,
ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. an association of persons or a body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. any agency, office or branch owned or controlled by any of the above persons (i to vi).

m. "Politically Exposed Persons" are individuals who are or have been entrusted with prominent public functions in India or abroad i.e. Heads of States/Government, senior politicians, senior government/judicial/military officers, senior executive of state-owned corporations, important political party officials etc.

n. "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:

i. 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
ii. appears to be made in circumstances of unusual or unjustified complexity; or
iii. appears to not have economic rationale or bona-fide purpose; or
iv. 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.

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

i. opening of an account;
ii. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
iii. the use of a safety deposit box or any other form of safe deposit;
iv. entering into any fiduciary relationship;
v. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
vi. Establishing or creating a legal person or legal arrangement.

p. "Video-based Customer Identification Process (V-CIP)" is 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 Customer KYC.

q. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Master Direction - Know Your Customer (KYC) Direction, 2016 as amended from time to time.

4. Designated Director and Principal Officer

a. The Director of the Company Mrs. Monica Sanket Khemuka shall be appointed as Designated Director for ensuring compliance with the obligations under PMLA, 2002.

b. The Compliance Officer Mr. Shubham Rajesh Agrawal shall act as the Principal Officer of the Company for the purpose of KYC / AML matters and who will be responsible for implementation of and compliance with this policy. His duties, in this regard will be as follows:

i. overall monitoring and compliance of KYC/AML Policy
ii. monitoring and reporting of transactions and sharing of information as required under the law.
iii. timely submission of Cash Transaction Reports (CTR's), Suspicious Transaction Reports (STR) or any other applicable reports to FIU-IND
iv. submission of periodical reports to management
v. Customer Acceptance Policy
vi. Money Laundering and Terrorist Financing Risk Assessment as per Clause 5A of the RBI-KYC Directions

5. Customer Acceptance Policy

a. The Customer Acceptance Policy lays down explicit criteria for acceptance of customers. The Policy ensures that the following procedures shall be followed in relation to customers who approach for availing financial facilities with the Company. The criteria laid down are:

i. No account is opened in anonymous or fictitious names or on behalf of other persons whose identity has not been disclosed or cannot be verified.
ii. Parameters of risk perception are clearly defined in terms of nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status.

iii. Customers would be categorised as low, medium and high risk.

iv. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

v. Not to open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e. company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the company.

vi. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there would be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

vii. Necessary checks will be done before opening a new account so as to 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.

viii. The nature and extent of due diligence will depend on the risk perceived by the company. However, while preparing customer profile, branches/offices should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

ix. A system is required to be put in place for 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. Such review of risk categorization of customers should be carried out at regular intervals as prescribed by Risk Department of the company.

x. 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.

6. Customer Identification Procedure

a. Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. NFPL will obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship.

b. The first requirement of customer identification procedures to be satisfied is that a prospective customer is the person who he/she claims to be.

c. The second requirement of customer identification procedures is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected or predictable pattern of transactions.

d. Identity shall be verified for: -

i. The named account holder;

ii. Beneficial owners;

iii. Signatories to an account; and

iv. Intermediate parties.

e. The Customer Identification Procedures are to be carried out at the following stages:

i. While establishing a new business relationship; or

ii. Periodically as part of KYC review or when the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

f. Copies of the documents produced as Proof of Identity and Address shall be obtained and retained with the NFPL, wherein a responsible Company Official has to attest such copies certifying that the Originals thereof have been verified.

g. The periodicity of updating of customer's identification data should be done once in 10 years in case of low-risk category customers, once in 8 years in case of medium risk category customers and once in 2 years in case of high-risk categories.

h. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

i. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure-B.

j. Also, the information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes. It will be ensured that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his /her consent and after opening the account.

k. **Customer Due Diligence (CDD):** Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

l. Accounts opened using OTP based e-KYC shall not be allowed for more than 1 year unless identification or V-CIP is carried out

m. If Aadhaar details are used for V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

n. 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.

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

iii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication shall be subject to conditions laid down in Master Directions, updated from time to time.

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

o. While undertaking V-CIP, NFPL shall adhere to minimum standards as mentioned in Annexure C.

p. In case the CDD is outsourced, then the records or the information of the customer due diligence carried out by the third party should be obtained within reasonable time from the third party or from the Central KYC Records Registry.

q. In case the CDD is outsourced, the decision-making functions of determining compliance with KYC norms should not be outsourced.

r. CDD procedure should be applied at the UCIC level and if an existing KYC complaint customer of NFPL desires to open another account, there shall be no need for a fresh CDD exercise.

s. NFPL can establish relationship with Politically Exposed Persons (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; senior level for this purpose shall include HOD & above.

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; the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

7. Risk Management

a. The Company shall adopt a risk-based approach to ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. Company will adhere to the following for effective implementation of Risk Management:

i. Originals of the KYC documents shall be verified by officials of the Company and copies thereof shall be obtained and retained with the Company. Such copies shall be attested by the Company officials certifying that they have been verified with the originals.

ii. KYC documents so obtained shall be properly arranged and filed in order so that they shall be available for verification any time.

iii. Company shall ensure an independent evaluation of compliance of KYC/AML policy including legal and regulatory requirements. They shall report Lapses observed in this regard as Irregularities in their Audit Reports.

iv. Adverse features noted shall be brought to the attention of the Principal Officer.

v. Summary of serious Irregularities/deviations shall be placed before the Audit Committee of the Board at quarterly intervals.

vi. Review of implementation of KYC/AML guidelines shall also be placed before the Audit Committee of the Board by the Principal Officer at quarterly intervals.

vii. The Company shall have an on-going employee training programme so that members of the staff are adequately trained in KYC/AML procedures.

viii. The Principal Officer designated by the Company in this regard shall have responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML Policy.

ix. Designated Director shall be responsible for the overall compliance with the obligations under the respective applicable Act and Rules.

8. Risk Categorisation

a. The Company shall categorize its customers based on the risk perceived by the Company. The level of Categorisation would be Low risk, Medium Risk and High risk.

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 clients' business and their location etc.

c. For the purpose of risk Categorisation, individuals and entities whose identity and source of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Examples of low-risk customers would be people belonging to lower economic strata of the society whose accounts show small balances and low turnover, government departments, government owned companies, statutory bodies, and salaried individuals.

d. Customers who are likely to pose higher than average risk to the Company would be categorized as medium or high risk. While categorizing the customers are medium or high-risk due consideration would be given to the customer's background, nature of the activity, country of origin, profile, etc. In such cases, Company will apply higher due diligence measures keeping in view the risk level. Examples of the customer requiring higher due diligence may include non-resident customers, trusts, societies, charitable organisations, non-face to face customers, those with dubious reputations as per public information available etc. Characteristics of High Risk and Medium Risk Customers are given as Annexure A.

e. Special care and due diligence shall be exercised in case of individuals who happen to be Politically Exposure Persons (PEP). PEP are individuals who are or have been entrusted with prominent public functions within or outside the country like Heads of state and

Government, senior politicians, senior government/judicial/military officers, senior executive of state-owned corporations, important political party officials etc.

f. Full KYC exercise will be required to be done at least every 2 years for high-risk individuals and entities.

g. Full KYC exercise will be required to be done at least every 8 years for medium risk and at least every 10 years for low-risk individuals and entities taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

h. If an existing KYC compliant customer desires to open another account with the Company, there should no need for submission of fresh proof of identity and/or proof of address for the purpose.

i. Fresh photographs will be required to be obtained from minor customer on becoming major.

9. Monitoring of Transactions:

a. Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent logical or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

b. After due diligence at the appropriate levels in the company, transactions of suspicious nature and/or any other type of transaction notified under PML Act, 2002 will be reported to the appropriate authority and a record of such transaction will be preserved and maintained for a period as prescribed in the Act.

10. Beneficial Ownership

a. The Company shall determine the beneficial ownership and controlling interest in case of the customers who are not individuals and the KYC of the beneficial owners will be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice. The guideline applicable for beneficial ownership is given as Annexure A.

11. Unique Customer Identification Code

a. Every customer should be provided with a Unique Customer Identification Code. This will help to identify customers, track the facilities availed, monitor financial transactions and enable the Company to have a better approach to risk profiling of customers.

12. Internal Control System

a. The Company's Internal 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.

b. The Management under the supervision of Board shall ensure that the audit function is staffed adequately with skilled individuals. The management will specifically check and verify the application of KYC procedures at the office and comment on the lapses observed in this regard.

c. The compliance in this regard shall be put up before the Audit Committee of the Board along with their normal reporting frequency.

d. Further, the Company (or any such department duly appointed by the management) shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel called as the KYE (Know Your Employee) so as to ensure that

Persons of criminal nature/ background do not get an access, to misuse the financial channel.

13. Record Management

a. The Company shall:

i. maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least 5 years from the date of transaction;

ii. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least 5 years after the business relationship is ended;

iii. make available the identification records and transaction data to the competent authorities upon request;

iv. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005) mentioned as below:

a) All cash transactions of the value of more than Rs.10 lakhs or its equivalent in Indian currency, though by policy the Company does not accept cash deposits in foreign currency shall be supported by the PAN of the customer.

b) PAN number to be collected by the Company for all series of cash transactions integrally connected to each other which have been valued above Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

c) All transactions involving receipts by non-profit organizations of Rs.10 lakhs or its equivalent in foreign currency.

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

e) All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

v. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

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.

vi. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

vii. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

14. Customer Education

a. The Company recognizes the need to spread the awareness of KYC and AML measures and the rationale behind them amongst the customers. Appropriate measures will be taken by the Company in this regard.

15. Periodic Updation (KYC in Existing Accounts)

Periodic updation of KYC documents needs to be done for the following types of customers:

i. High risk- at least once in every two years

ii. Medium risk- once in every five years

iii. Low risk- once in every ten years as per the following procedure:

a) PAN verification from the verification facility available with the issuing authority and

b) Authentication, of Aadhaar Number already available with the NFPL with the explicit consent of the customer in applicable cases.

c) In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.

d) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized as 'low risk'. In case of low-risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

iv. In case of Legal entities, RE shall review the documents sought at the time of opening of account and obtain fresh certified copies.

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

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

Provided that the company shall ensure that the prescribed KYC documents are available with them.

16. Introduction of New Technologies

a. Company will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent misuse of technology innovations for money laundering activities. Company will ensure that appropriate KYC procedures are duly applied to customers using new technology driven products.

17. Persons Authorised

a. The Company shall accept full consequences of any violation by the persons authorised by the Company including brokers/agents etc. who are operating on its behalf.

18. Prevention of Money Laundering Act, 2002 – Obligations of Company in terms of rules notified thereunder:

a. The Company has appointed "Principal Officer" as per clause 4 above, who will put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. Further with the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

i. *issue a warning in writing; or*

ii. *direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or*

iii. *direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or*

iv. *by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."*

For the purpose of this policy document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of funds.

b. Money Laundering - Risk Perception:- Following are the risks, which arise out of Money Laundering activities:

i. Reputation Risk - Risk of loss due to severe impact on reputation. This may be of particular concern given the nature of business, which requires the confidence of customers, and the general market place.

ii. Compliance Risk - Risk of loss due to failure of compliance with key regulations governing the operations.

iii. Operational Risk - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

iv. Legal Risk - Risk of loss due to any legal action on the company or its staff may face due to failure to comply with the law.

v. Company should ensure to cover all the above stated risks and should have proper checks to control to combat the above stated risks.

c. Maintenance of Records of Transactions and Preservation

i. There will be a system of maintaining proper record of transactions prescribed under PMLA, 2012 and PML Rule 2005 in prescribed format. The same along with KYC documents should be preserved for prescribed period. The Company will hire vendors where the physical copies will be preserved and also important data will be kept online on computer servers.

d. Reporting to Financial Intelligence Unit - India

i. Company will abide the PMLA rules for reporting information pertaining to cash and suspicious transactions to the specified authorities post conducting due enquiries. As a part of transaction monitoring mechanism, systems/ processes will be put in place to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

ii. The periodical reporting to FIU will be done regularly in soft copy through online mode. For e.g. CTR filed online on FIU website on regular basis.

e. Suspicious Transaction Monitoring and Reporting

i. NBFCs are required to file reports on suspicious transactions with financial intelligence unit – India (FIU), as per the prevention of Money Laundering Act (PMLA), within seven days of a transaction getting identified as a suspicious transaction by the principal officer (PO). The suspicious transaction is defined by RBI as a transaction, including as attempted transaction, whether or not made in cash, which to a person acting in good faith:

ii. 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

iii. Appears to be made in circumstances of unusual or unjustified complexity; or

iv. Appears to not have economic rational or bona – fide purpose; or

v. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

f. Monitoring and Reporting of Suspicious transaction activity

i. The Company will keep a continuous vigil with regards to customer's behaviour or approach while dealing with the company. The company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose.

ii. In case any usual act or event or behaviour is noticed in relation to customer, the same shall be investigated and if required report as suspicious activity. The staff of branches / department should observe the traits of customer that raise suspicion. List of suspicious transactions to be tracked is given below:

a) Reluctance on part of the customer to provide confirmation regarding his identity, nature of business, business relationship, officers or directors or its locations

b) KYC documents provided by the customer are forged, fabricated or altered

c) KYC documents provided by the customer cannot be verified (e.g foreign documents)

d) Forged documents provided by the customer (e.g. fake title deeds)

e) Difficulty in identifying beneficial owner of the transaction

f) Nature of transaction under taken by the customer is too complex or the customer is not able to explain the source of funds

g) Nature of transaction undertaken by the customer does not justify his nature of business or lifestyle or standard of living

h) Customer has limited or no knowledge about the money involved in transaction or conducting transaction on behalf of someone else

i) Customer is investigated for criminal offence by law enforcement agency

j) Customer is investigated for terrorist financing or terrorist activities

k) Adverse media report about the customer

l) Negative Information about the customer received from any other financial institution (e.g. Fraud etc)

m) For all part prepayments/ foreclosures which are not balance transfer (BT) involving Rs. 0.50 Crores. Or above should be reviewed through customer service and reported to Principal Officer. The concerned team shall review whether same is suspicious or not and accordingly Principal Officer shall report the same if required.

iii. Any enquiry from CBI, Police, Enforcement Directorate, Department or Vigilance and Anti-corruption, Income Tax or Service tax authorities etc. on the statement of account of the customer should result in STR.

g. Monitoring and Reporting of Cash Transactions

i. In case of repayment, no cash of Rs. 50,000/- and above shall be accepted from a Customer/ any other intermediary (auction cases) without obtaining a copy of the PAN card of the Customer/any other intermediary. In case a customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

ii. Any cash transactions of Rs. 10 lakhs and above and integrally connected cash transactions of Rs. 10 lakh and above per month shall be reported to FIU-IND by 15th of the succeeding month as CTR. For further details, Rules 3 to 8 (Appendix B) may be seen.

iii. The Company shall lay down proper mechanism to check any kind of attempts to avoid disclosure of PAN details. In case of possible attempts to circumvent the requirements, the same shall be reviewed from the angle of suspicious activities and shall be reported to FIU-IND, if required.

19. Central KYC Records Registry

a. The Government of India has authorized the Central Registry of Securitisation Asset Reconstruction and Security Interest of India, to act as, and to perform the functions of the CKYCR.

b. In terms of provision of Rule 9(1A) of PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer. The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The Company shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI. Once KYC Identifier is generated by CKYCR, REs shall ensure that the same is communicated to the individual/LE as the case may be.

c. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to April 1, 2017, and April 1, 2021 respectively at the time of periodic updation as specified in the Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

d. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

i. there is a change in the information of the customer as existing in the records of CKYCR;

ii. the current address of the customer is required to be verified;

iii. the RE considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

20. Combating financing of Terrorism

a. Company shall institute suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

b. Before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs).

c. It would be necessary that adequate screening mechanism is put in place by Company as an integral part of their recruitment/hiring process of personnel.

d. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions.

21. Requirements/obligations under International Agreements Communications from International Agencies

a. Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

b. 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.

c. 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 freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967. The procedure laid down in the UAPA Order (Annex I of this Master Direction shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

22. Other Instructions

a. Secrecy Obligations and Sharing of Information:

i. Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

ii. While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

iii. The exceptions to the said rule shall be as under:

a) Where disclosure is under compulsion of law,

b) Where there is a duty to the public to disclose,

c) the interest of the company requires disclosure and

d) Where the disclosure is made with the express or implied consent of the customer.

iv. Company shall maintain confidentiality of information as provided in Section 45 NB of RBI Act 1934.

Annexure-A

Indicative list for risk categorization

High Risk Customers

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
- 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;
- Individuals and entities in watch lists issued by Interpol and other similar international organizations;
- Customers with dubious reputation as per public information available or commercially available watch lists;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- 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.;
- Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
- Non-face-to-face customers;
- High net worth individuals;
- Firms with 'sleeping partners';
- Companies having close family shareholding or beneficial ownership;
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- 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;
- Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the Company;
- Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.;
- Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations;
- Gambling/gaming including "Junket Operators" arranging gambling tours;
- Jewelers and Bullion Dealers;
- 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);
- Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;
- Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
- Customers that may appear to be Multi-level marketing companies etc; - Individual who is a prisoner in jail.
- Jewelers – Bullion dealers

Medium Risk Customers

- Stock brokerage;
- Import / Export;
- Gas Station;
- Car / Boat / Plane Dealership;
- Electronics (wholesale);
- Travel agency;
- Telemarketers;
- Providers of telecommunications service, internet café, International direct dialing (IDD) call service

Low Risk Customers-

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.

Annexure-B

List of KYC documents for a different type of customers

Sr. No.	Individual / Type of Entity (features to be verified)	Documents required
1.	Individuals	Permanent Account Number (Mandatory) (the same shall be verified from the verification facility of the issuing authority including through DigiLocker) AND Any one of the OVD (Proof of Identity and Address) AND One recent photograph **List of OVD:** a. the passport, b. the driving licence, c. Proof of possession of Aadhaar number, d. the Voter's Identity Card issued by the Election Commission of India, 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 and address. 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. 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. 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; 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; Customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

2.	Proprietorship Matters	Documents or equivalent e-documents which could be obtained as proof of business/activity for proprietary firms (any two) in additions to the documents of the proprietor as individual: a. Registration certificate b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act. c. Sales and income tax returns. d. GST certificate (provisional / final) e. Certificate /registration document issued by Sales Tax/Professional Tax authorities. f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. h. Utility bills such as electricity, water, and landline telephone bills, etc. i. In cases where the Company is satisfied that it is not possible to furnish two such documents, it may, at their discretion, accept only one of those documents as proof of business/activity. Provided that it undertakes contact point verification and collects such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
3.	Company Name of the Company Principal place of business & Mailing Address	Certified copies of following documents or equivalent e-documents should be obtained: a. Certificate of incorporation b. Memorandum and Articles of Association

4.	Telephone No.	Permanent Account Number of the company a. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf. Individual KYC of person authorised to transact on behalf of the company.
5.	Partnership Firms Legal Name Address Names of all partners and their address Telephone No.	Certified copies of following documents or equivalent e-documents should be obtained: a. Registration certificate b. Partnership deed c. Permanent Account Number of the partnership firm d. Individual KYC of person authorised to transact on behalf of the firm
6.	Trust Name of Trust/ Trustees/Settlers/ beneficiaries/Signatories/founders Telephone No.	Certified copies of following documents or equivalent e-documents should be obtained: a. Registration certificate b. Trust deed c. Permanent Account Number or Form No.60 of the trust d. Individual KYC of person authorised to transact on behalf of the firm
7.	Unincorporated Association / Body of Individuals (Includes Unregistered Trusts / Partnership Firms / Societies)	Certified copies of following documents or equivalent e-documents should be obtained: a. Resolution of the managing body of such association or body of individuals b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals c. Power of attorney granted to transact on its behalf d. Individual KYC of person authorised to transact on behalf of the firm e. Any other information/document as may be required to collectively establish the legal existence of such an association or body of individuals.
8.	Others	For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or equivalent e-documents shall be obtained: a. Document showing name of the person authorised to act on behalf of the entity; b. Individual KYC of person authorised to transact on its behalf c. Any other information/document as may be required to establish the legal existence of such an entity/juridical person

Annexure-C

Digital KYC Process

A. The company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the company.

B. 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 the company to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the company or vice-versa. The original OVD shall be in possession of the customer.

D. 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 customer.

E. 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 colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. 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 water-marking 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.

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

H. 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.

I. 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 officer registered with the RE 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.

J. 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.

K. 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.

L. 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.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the RE 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.

LIST OF ABBREVIATIONS

1. AML: Anti-Money Laundering
2. BT: Balance Transfer
3. CTR: Cash Transaction Reports
4. CVC: Card Verification Code
5. CBI: Central Board of Investigation
6. CERSAI: Central Registry of Securitisation Asset Reconstruction and Security Interest of India
7. CKYCRR: Central KYC Records Registry
8. Crs.: Crores
9. Etc.: Etcetera
10. FIU: Financial Intelligence Unit
11. NFPL:Neuzen Finance Private Limited
12. i.e.: For example
13. KYC: Know Your Customer
14. NBFC: Non-Banking Financial Company
15. No.: Number
16. NRI: Non-Resident Indian
17. OVD: Officially Valid Document
18. PAN: Permanent Account Number
19. PO: Principal Officer
20. PPO: Pension Payment Orders
21. PEP: Politically Exposed Persons
22. RBI: Reserve Bank of India
23. RE: Regulated Entities
24. STR: Suspicious Transaction Reports
25. &: And