

FINQUEST FINANCIAL SOLUTIONS PRIVATE LIMITED

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

Finquest Financial Solutions Private Limited

CIN: U74140MH2004PTC146715

Registered Address: 602, Boston House,
6th Floor, Suren Road, Andheri (E),

Mumbai-400093

Email Id: hpatel@finquestonline.com

Version / Annual Review Details :

Particulars	Date	Version No.
Adopted in the Board Meeting held on	02/02/2017	V. 1
Revision in the Board Meeting held on	29/03/2022	V. 2
Revision in the Board Meeting held on	02/03/2023	V. 3

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

PREAMBLE

The Reserve Bank of India (RBI) has issued Master Direction on Know Your Customer (KYC) Direction, 2016 in terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 ('Master Direction') for Regulated Entities (REs) which includes Non- Banking Financial Companies (NBFCs).

In accordance with the provisions of the Master Direction, Finquest Financial Solutions Private Limited (the Company / FFSP) being an RBI registered Non- Banking Financial Company (NBFC) and a "Regulated Entity", the Company has adopted the following KYC guidelines with suitable modifications depending on the business activities undertaken by the Company. The Company has ensured that a proper policy framework on KYC and AML measures are formulated in line with the prescribed Master Direction and has put in place a policy framework duly approved by its Board of Directors ('Board'). The Company shall also ensure that the information collected from the customer for the purpose of opening of account shall be kept as confidential and any details thereof shall not be divulged for cross selling or any other purposes.

In accordance with the directives from the RBI, the Company has framed the Policy on Know Your Customer and Prevention of Money Laundering Activities ('KYC and PMLA Policy/ Policy') which is stated hereunder.

The RBI vide the Master Direction and subsequent modifications thereof, has also prescribed 'Anti Money Laundering' guidelines/ standards, applicable to NBFCs. In view of the same, the Policy shall broadly also achieve the following purposes:

- Prevent criminal elements from using the Company for money laundering activities;
- Enable Company to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently;
- Put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
- Comply with applicable laws and regulatory guidelines;
- Ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

As per the Master Directions, the Policy has the following four key elements:

- i. Customer Acceptance Policy;
- ii. Risk Management;
- iii. Customer Identification Procedures (CIP); and
- iv. Monitoring of Transactions.

Central KYC Registry: With reference to the directives of the RBI on CKYC Registry advising inter-alia NBFCs to upload the KYC data with CKYC Registry in respect of new individual loan accounts, the Company has prepared a detailed plan for uploading the KYC data on CKYC Registry which forms part and parcel of this Policy.

Review of the Policy: The Board of Directors of the Company (the Board) will review the Policy adopted for KYC and AML from time to time and recommend incorporation of suitable modifications / changes. Any modifications in the Policy as a result of the change in the RBI guidelines, will be incorporated as required under the statute. All such changes /modifications will be reported to the Board for approval.

Procedures and Manuals: The Company shall formulate business/product specific risk profile of the customer and lay down procedures and manuals for compliance of this Policy.

APPLICABILITY

The Policy shall be equally applicable to the persons authorised by the Company including brokers/agents etc. transacting on behalf the Company.

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

DEFINITIONS

In this Policy, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

Act	Shall mean the Prevention of Money-Laundering Act, 2002 and subsequent amendments thereto
Beneficial Owner (BO)	refers to the natural person(s) who ultimately owns or controls a customer and/ or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Board/ BoD	Shall mean Board of Directors of the Company
Certified Copy	Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number (where offline verification cannot be carried out) or any other OVD produced by the customer, with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the KYC Directions.
Company	Shall mean Finquest Financial Solutions Private Limited
Customer	Shall mean any person, as defined in the RBI’s Master Directions on ‘Know Your Customer’ and Anti-Money Laundering Measures, as amended from time to time. For the purpose of clarification, it may be noted that “Customer” means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
Digital KYC	Shall mean the process of 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 the authorized officer of the Company, in accordance with provisions of the Act

KYC Directions	Shall mean Master Direction - Know Your Customer (KYC) Direction, 2016 issued by the RBI as amended from time to time
Equivalent e- document	Shall mean 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.
Officially Valid Document (OVD)	Shall mean the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.
Policy	Shall mean this KYC and PMLA Policy formulated by the Company
Rules	Shall mean Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and subsequent amendments thereto.
Senior Management	Shall mean personnel of the Company who are members of its core management team excluding the Board, comprising all members of the executive committee of the Company, including the functional heads;
Unique Customer Identification Code (UCIC)	Shall mean a unique code provided by the Company to each Customer while entering into an account-based relationship with the Customer in order to maintain identification records at person/Customer level
V-CIP	Shall mean the process of Customer identification, by undertaking seamless, secure, real-time, consent based audio-visual interaction with the Customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the Customer.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, RBI Master Direction on Know Your Customer (KYC) Direction, 2016 any statutory modification, amendment or re-enactment thereto or as amended from time to time or as used in commercial parlance, as the case may be.

POLICY OUTLINE

Specifying the 'Senior Management' for the purpose of KYC Compliance:

The Board has identified Risk and Compliance Head as the Senior Management who shall be responsible for ensuring compliance with the Policy and the guidelines/ directions issued by RBI from time to time.

Allocation of responsibility for effective implementation of policies and procedures:

The operations team of the Company shall be responsible for ensuring the effective implementation of this Policy and the procedures laid herein.

Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements:

The Senior Management shall carry out regular evaluation of the compliance functions prescribed under this Policy and guidelines/ Master Directions issued by the RBI in this regard, as amended from time to time. Any non-compliance or deviation shall accordingly be reported to the Board.

Internal audit system to verify the compliance with KYC/AML policies and procedures:

The Board or any other committee to whom the power has been delegated by the Board shall carry out concurrent/ internal audit on a quarterly basis, to verify the compliance with this Policy and procedures laid herein.

Submission of quarterly audit notes and compliance:

The aforesaid audit report shall thereafter be submitted to the Board or Audit Committee, as the case may be, for their review and comments.

CUSTOMER ACCEPTANCE POLICY

Customer Acceptance Policy (CAP) lays down the criteria for acceptance of Customers. The guidelines in respect of the Customer relationship with the Company are broadly stated below:

- a. The Company shall not open an account in cases where it is unable to carry out appropriate Customer Due Diligence (CDD) measures due to non-cooperation by the Customer or non-reliability of the documents/ information furnished by him/her. CDD means identifying and verifying the Customer and the BO using 'Officially Valid Documents' (OVD) as a 'proof of identity' and a 'proof of address'.
- b. No account shall be opened by the Company in anonymous or fictitious/benami names.
- c. Accept Customers only after verifying their identity, as per CDD Procedures defined aforesaid and shall be followed for all the joint account holders (including guarantors) as well, while opening a joint account. No Account shall be opened where the Company is unable to apply appropriate Customer due diligence (CDD) measures, either due to non-cooperation of the Customer or non-reliability of the documents/information furnished by the Customer.
- d. No transaction or account based relationship to be undertaken without following the CDD procedure.
- e. In the event, the Customer is permitted to act on behalf of another person/entity, the Company shall verify that the Customer has the necessary authority to do so by scrutinizing the authorizing document/s.
- f. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation shall be as specified by the Policy and as amended or specified from time to time. Any exceptions shall be discussed / informed with the Principal Officer.

g. If the Customer or the Beneficial Owner is Politically Exposed Person, then the same shall be specifically highlighted to the Principal Officer for their approvals.

h. 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. Implementation of CAP should not become too restrictive and result in denial of the services to the general public, especially to those who are financially or socially disadvantaged.

i. The Company shall seek only such information from the Customer which is relevant to the risk category, is not intrusive and is in conformity with the guidelines issued in this regard from time to time. Any other information from the Customer should be sought separately with his/her consent and after opening the account.

j. United Nations Security Council (UNSC) Lists: If the name of the Customer entity/individuals appears on the following two lists of individuals and entities, suspected of having terrorist links, no account shall be opened by the Company.

The details of the two lists are as given below:

ISIL (Da'esh) & Al-Qaida Sanctions List: which includes names of individuals and entities and other groups associated with the Al-Qaida. The updated ISIL & Al Qaida Sanctions List is available at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

1988 Sanctions List: consisting of individuals (Section A of the consolidated list) and entities and other groups (Section B) associated with the Taliban which is available at <https://www.un.org/securitycouncil/sanctions/1988/materials>

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

k. CDD procedure shall be followed for all co-borrowers while entering into a co-borrowing transaction.

RISK MANAGEMENT

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

a) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Company;

b) Risk categorization shall be undertaken based on parameters such as Customer's identity, social/financial status (such as net-worth, turnover, income source), nature of business activity, and information about the clients' business and their geographic 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 behaviour for risk management and suitable timely corrective action.

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

e) The risk categorization would be reviewed and enhanced due diligence measures would be applied in the case of a higher risk perception of a Customer. High-risk accounts of the Company shall be subjected to more intensified monitoring and shall be reviewed at least once in every six months.

(i) High Risk – (Category A):

High risk Customers typically will include:

a) Individuals and entities listed or identified in – various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267, schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.;

b) Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the Customer, frequent and unexplained movement of accounts to different institutions, etc.;

c) Non – resident Customers (excluding applicants for retail education loans)

d) High net worth individuals without an occupation track record of more than 3 years

e) Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (Excluding applicants / Beneficial Owners who are running affiliated education institutions) – Refer Annexure I

f) Firms with sleeping partners

g) Politically exposed persons (PEPs) of Indian/ foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate Beneficial Owner

h) Customers with dubious reputation as per public information available or commercially available watch lists.

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

j) Jewellers and Bullion Dealers;

k) Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);

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

m) Customers that may appear to be Multi-level marketing companies etc.

n) Any borrower/co-borrower working in a country identified as high risk.

(ii) Medium Risk – (Category B):

Medium risk Customers typically will include:

a) Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (i.e. applicants / Beneficial Owners who are running affiliated education institutions)

b) Salaried applicant with variable income/ unstructured income receiving Salary in cheque

c) Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialling (IDD) call service.

d) Self employed professionals other than HNIs (excluding applicants for retail education loans)

e) High net worth individuals with occupation track record of more than 3 years

f) One of more borrowers resident outside India (excluding student going abroad to study)

g) Companies having close family shareholding or Beneficial Ownership.

h) Non face to face to Customers, or Customer outside the state of operation for the Company(Refer Annexure I)

(iii) Low Risk – (Category C):

Low risk Customers typically will include:

a) Salaried employees with well defined salary structures

b) People working with government owned companies, regulators and statutory bodies, etc.

c) People belonging to lower economic strata of the society whose accounts show small balances and low turnover

d) People working with Public Sector Units

e) People working with reputed Public Limited Companies and Multinational Companies

f) All borrowers resident in India (including student going abroad to study)

g) Low risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories.

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

CUSTOMER IDENTIFICATION PROCEDURE

Customer identification shall be undertaken at the time of commencement of an account-based relationship which would include identifying its Customers, verifying their identity and KYC documents, obtaining information on the purpose and intended nature of the business relationship; and determining whether a client is acting on behalf of a Beneficial Owner, and identifying the Beneficial Owner in accordance with the Master Directions read with the PML Act and Rules and take all steps to verify the identity and KYC documents of such Beneficial Owner.

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

a. Commencement of an account-based relationship with the Customer;

b. When there is a doubt about the authenticity or adequacy of the Customer identification data it has obtained;

c. Selling their own products, selling third party products as agents and any other products;

d. Carrying out transactions for a non-account based Customer (walk-in Customer).

2. The Company shall obtain satisfactory evidence of the identity of the Customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.

3. The Company shall obtain Permanent Account Number (PAN) of the Customers as per the applicable provisions of the Income Tax Act, 1961 and the Rules made thereunder and as amended from time to time and in case of persons who do not have PAN, the Company shall collect Form 60 from such persons.

4. For the Customers that are legal person or entities:

i. the Company will verify the legal status for the legal person/ entity through proper and relevant documents;

ii. the Company will understand the beneficial ownership and control structure of the Customer and determine who the natural persons are and who ultimately controls the legal person.

5. Additional documentation may be obtained from the Customers with higher risk perception as may be deemed fit. This shall be done having regard but not limited to location (registered office address, correspondence address and other addresses as may be applicable), nature of business activity, repayment mode & repayment track record.

6. For the purpose of verifying the identity of Customers at the time of commencement of an account-based relationship, the Company, at its discretion, rely on Customer due diligence done by a third party,

subject to the following conditions (However, the ultimate responsibility for CDD and undertaking enhanced due diligence measures, as applicable, will be with the Company and decision-making functions of determining compliance with KYC norms shall not be outsourced):

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 per **Annexure I**), as applicable, will be with the Company.

7. The Company/authorized representative of the Company shall verify the identity of the Customer with the proof of identity submitted by him/her. Further, the PAN details shall be verified from the database of the issuing authority.

8. Further, the authenticity of the permanent address provided in the application form shall be established by matching the same with OVDs submitted by the Customer.

9. If the OVD does not contain updated address of the Customer, a proof of updated address such as a utility bill (not more than 2 months old), property or municipal tax receipt, pension or family pension payment orders (PPOs) or other documents as mentioned in the KYC Directions shall be obtained from the Customer, which shall be deemed to be OVD for the purpose of serving as a proof of address.

10. Further, in the Company shall obtain from the Customer, an OVD with updated address within three months of submitting the aforementioned documents.

11. The authorized representative also would have the process of allotting a UCIC for easy identification of all the relationships of any Customer with the Company. The UCIC shall not just act as a reference number but serve the purpose of assigning a unique ID at customer-level, *inter-alia* for easy identification of all the relationships of the particular Customer with the Company.

12. Information collected for the purpose of opening an account would be kept as confidential and would not be divulged to outsiders for cross selling or any other purpose other than for the statutory requirement of sharing the Customer account details with at least all the Credit Information Companies (CICs) approved by RBI. Information sought from the Customer would be relevant to the perceived risk and would not be intrusive.

13. If the OVD submitted by the Customer at the time of KYC includes both address and identity proof then he is not required to submit additional OVD.

14. In case it is observed that the address mentioned as per 'proof of address' has undergone a change, Company shall ensure that fresh proof of address is obtained within a period of six months.

15. Documentation requirements and other information is 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 RBI from time to time.

16. Where the Company undertakes the physical KYC process, it shall obtain Certified Copies of the OVD. Further, 'originally seen and verified' (OSV) stamp with signature of the Company official/agent is also placed on the KYC document.

16. In case the Company undertakes Digital KYC process or V-CIP process, it shall ensure that the same is in compliance with the KYC Directions.

17.

The Company may also obtain KYC identifier of the Customer and download the proof of identity and address from the Central KYC Registry (CKYCR portal). The downloading of OVDs from the CKYCR portal shall suffice the need of verification. However, further due diligence shall be carried out by the Company.

18. 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 not the address where the Customer is currently residing, a declaration shall be taken from the Customer about her/ his local address on which all correspondence will be made by the Company. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as cheque books, ATM cards, telephonic conversation, positive address verification, Rent agreement, etc.

19. Enhanced Due diligence measures are indicated in **Annexure I**.

20. An indicative list of the nature and type of documents/information that may be relied upon for customer due diligence / identification is given in **Annexure II**. It shall be ensured that the KYC documents are obtained, verified and the loan agreement is duly executed before establishing any account relationship with the Customer and disbursal of loan amount.

8. Periodic Updating of KYC data:

The Company shall periodically update the Customer's KYC information / documents after the transaction is entered. The periodicity of updating of Customer's KYC data shall be once in 10 years for low risk Customers, once in every 8 years for medium risk Customers, and once in 2 years for high risk categories, subject to following conditions:

- i. Fresh proofs of identity and address shall not be sought at the time of periodic updation from Customers who are categorized 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.
- ii. 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.
- iii. Physical presence of low risk Customer at the time of periodic updation shall not be insisted upon.
- iv. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.
- v. Fresh photographs shall be obtained from Customer for whom account was opened when they were minor, on their becoming a major.
- vi. E-KYC process using OTP based authentication for periodic updation is allowed provided while on boarding, the Customer was subjected to proper KYC process.

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

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

An indicative list of the nature and type of documents/information that may be relied upon for customer due diligence / identification procedure are stated in **Annexure-II**.

MONITORING OF TRANSACTIONS

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

As per Income Tax Act, 1961, for any Cash or its equivalent payment over and above Rs. 20,000/- (Rupees Twenty Thousand only), a 'source of funds' declaration for such cash should be obtained from the Customer/ person depositing / repaying the loan.

Note: Source of funds in cash is through 'sale of immovable property', then Cash or its equivalent for more than Rs. 20,000/- (Rupees Twenty Thousand only), shall not be accepted.

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. The Company shall make all endeavours to understand the normal and reasonable activity of the Customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. The Company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve cash over and above Rs. 1,00,000/- (Rupees One Lacs only) Rs. 1 lac shall particularly attract the attention of the Company. Higher risk accounts shall be subjected to intense monitoring.

The Company shall set key indicators for such account's basis the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. AFSL shall carry out the periodic review of risk categorization of transactions/Customer's accounts and the need for applying enhanced due diligence measures at a periodicity of not less than once in six (6) months.

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

The extent of monitoring an account shall be aligned with the risk category of the Customer. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the Customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Further, the Company shall maintain audit trails and adequate documentation for the above monitoring.

TRAINING PROGRAMME

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

Training requirements will have different focuses for frontline staff, compliance staff and officer/ staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

INTERNAL CONTROL SYSTEM

The Company will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management under the supervision of Board shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT:

The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc, in accordance with the following:

The periodicity of risk assessment exercise shall be determined by the Board, in alignment with the outcome of the risk assessment exercise. However, the same shall be reviewed at least annually.

The assessment process, as discussed below, should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

The risk assessment shall be properly documented.

The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.

The Company shall monitor the implementation of the controls and enhance them if necessary.

Process of Risk Assessment

The process of risk assessment by the Company may be divided into following stages:

Collection of Information: The Company shall prepare a database containing information of individuals with criminal background. The information for the database may be collected from various sources such as lists of terrorists provided by UN agencies, CBI, Enforcement Directorate etc. The database shall serve as a one-point collection of information relating to money laundering and terrorist financial risks and shall be updated from time to time, including information provided by RBI, if any.

Threat Identification: The Company shall then identify the threats arising due to the structure of its financial products. Such threats may arise due to no or less personal interface between the Company and the borrower, no/less physical examination etc.

Based on the database, the Company may identify the class of applicants or geographical regions from where there are higher risks of use of loan proceeds for terrorist purposes. It is also necessary to identify the source of funds of repayments by the borrowers. Based on relevant experience, the aforesaid list shall be updated from time to time.

Assessment of ML/TF vulnerabilities: Once the threats are identified, the extent of their impact on the Company shall be assessed on a regular basis. This shall be done by taking into consideration various factors such as nature, scale, diversity and complexity of the products, customer segments, number of customers and volume of transactions that may fall into identified risk categories, exposure of the Company to various jurisdictions (especially jurisdictions with relatively higher levels of corruption or organised crime), distribution channels (including the extent to which the Company deals directly with the customer or relies third parties to conduct CDD), reliability of internal audit findings etc. Such assessment shall be undertaken by [determine the responsible team/person] and the report of such assessment shall be submitted to the Risk Management Committee for review.

Analysis of ML/TF threats and vulnerabilities: Once threats and vulnerabilities are determined, the interplay between them shall be analysed by Risk Management Committee or Senior Management. The course of action and the decision to lend shall be based on the analysis of the extent of the risk that may arise owing to the threats and vulnerabilities.

Risk Mitigation: After conducting the analysis of threats and vulnerabilities, the Risk Management Committee or Senior Management of the Company shall determine the course of action to mitigate the risks. Areas or classes of applicants with higher risk may either be debarred from entering into any account-based relationship with the Company/the exposure to such classes may be limited or such classes shall be subject to additional scrutiny or both.

Further, the CDD procedure shall also be suitably amended in order to address such risks in the initial stages. The due diligence process may, when required, be divided into two parts, Enhanced Due Diligence for classes/applicants with high risk and Simplified Due Diligence i.e. the regular Due Diligence process of the Company for all classes of borrowers.

The Company may recruit suitable personnel/ or train the existing personnel to deal with such risks. The Company should have the ability to flag unusual movement of funds or transactions for further analysis. Further, it should have appropriate case management systems so that such funds or transactions are scrutinised in a timely manner and a determination made as to whether the funds or transaction are suspicious. The Company shall further ensure reporting of suspicious transactions and other specified transactions such as CTR, CBWTR etc. to FIU-IND as per the provisions of PML Act and rules. Further, the Company shall ensure to impart adequate training to the employees and staff to allow them to form sound judgments about the adequacy and proportionality of the AML controls.

Follow-up and maintaining up-to-date risk assessment: Transactions entered into with customers in risk classes shall be monitored more frequently than the others. Further, the database of information shall be kept up to date from time to time.

RECORD KEEPING

a) Maintenance of records of transactions

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

- i.** All cash transactions of the value of more than Rs. 2 lacs. Though as per the Policy the Company does not accept cash deposits / cash in foreign currency.
- ii.** All series of cash transactions integrally connected to each other which have been valued below Rs. 2 lacs where such series of transactions have taken place within a month.
- iii.** All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency.
- iv.** All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions;

v. records pertaining to identification of the Customer and his/her address; and

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

An Illustrative List of suspicious transaction pertaining to financial services / transactions are stated in **Annexure-III**.

b) Records to contain the specified information

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

i. the nature of the transactions;

ii. the amount of the transaction and the currency in which it was denominated;

iii. the date on which the transaction was conducted; and

iv. the parties to the transaction.

c) Maintenance and preservation of records

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

i. records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of Ten (10) years from the date of transactions between the clients and the Company.

ii. records of the identity of all clients of the Company is required to be maintained for a period of Ten (10) years from the date of cessation of transactions between the clients and the Company.

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

APPOINTMENT OF THE PRINCIPAL OFFICER

The Company shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Registered Office of the Company shall be responsible for ensuring compliance, monitoring and reporting of all transactions and sharing of information as required under the PMLA and the Rules made there under. The Principal Officer will report directly to the senior management or to the Board of Directors. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND at the time of appointment as well as any subsequent change.

The Principal Officer, under the supervision and guidance of the Designated Director, shall be responsible to ensure overall compliance specified under the Act and the Rules/ Regulations thereunder.

The Principal Officer would perform the following duties:

- i. Develop effective AML programs, including training programs
- ii. Assist the business in assessing how the system can be abused
- iii. Identify suspicious activity
- iv. Monitor implementation of this Policy
- v. Submit reports to statutory bodies and management

APPOINTMENT OF DESIGNATED DIRECTOR:

The Board of Directors shall nominate a “Designated Director” who shall be a person duly authorized by the Board to ensure compliance with the obligations prescribed by the Act and the Rules thereunder. It shall be ensured that the Principal Officer is not nominated as the “Designated Director”. The name, designation and address of the Designated Director shall be communicated to the FIU-IND at the time of appointment as well as any subsequent change.

REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA

In accordance with the requirements under PMLA, the Principal Officer of 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. An indicative list of suspicious transactions is stated in **Annexure III**.

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

CUSTOMER EDUCATION

Implementation of KYC procedures can sometimes lead to a lot of questioning by the Customer as to the motive and purpose of collecting such information. Therefore, the Company shall endeavour to take necessary steps, as may be required, to educate the Customer of the objectives of the KYC programme.

AUDIT

The Board of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensure their effective implementation;

Internal audit and compliance function would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of Company's own policies and procedures, including legal and regulatory requirements;

Internal Auditors shall check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard would be put up before the Audit Committee of the Board on quarterly basis;

The Company shall have an on-going employee training programme with different focuses for frontline staff, compliance staff and staff dealing with new Customers and educating them with respect to the objectives of the KYC Programme.

GENERAL

1. Closure of Accounts/Termination of Financing/Business Relationship

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 shall terminate Financing/Business Relationship after issuing due notice to the Customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Managing Director authorized for the purpose.

2. KYC for the Existing Accounts

While the KYC guidelines will apply to all new Customers, the same would be applied to the existing Customers on the basis of materiality and risk. However, transactions with existing Customers would be continuously monitored for any unusual pattern in the operation of the accounts.

3. Updation in KYC Policy of Company

The Principal Officer after taking the due approval from the Board of Directors of the Company shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

ANNEXURE – I

Enhanced Due Diligence (EDD) measures

1. Accounts of Politically Exposed Persons (PEPs)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

1.1 Branch/office shall gather sufficient information on any person/Customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

1.2 Branch/office shall verify the identity of the person and seek information about the sources of funds accounts of family members and close relatives of the PEP before accepting the PEP as a Customer.

1.3 The decision to provide financial services to an account for PEP shall be taken at a senior level and shall be subjected to monitoring on an ongoing basis.

1.4 The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

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

2.1 In the case of non-face-to-face Customers, apart from applying the usual Customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk. Further, the Company shall ensure that the first payment is to be effected through the Customer's KYC-compliant account with another RE, for enhanced due diligence of the non face to face Customers

2.2 Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for.

2.3 In the case of cross-border Customers, there is the additional difficulty of matching the Customer with the documentation and the NBFCs may have to rely on third party certification/ introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

3. Trust/Nominee or Fiduciary Accounts

The Company shall determine whether the Customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

The Company will take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation',

branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

4. Accounts of companies and firms



The Company will be vigilant against business entities being used by individuals as a front for maintaining accounts with the Company. The Company may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it shall not be necessary to identify all the shareholders.

ANNEXURE – II

Sr. No.	Type of Customers	Features to be verified	List of valid Documents
1	Individual	<p>Legal name and other names used</p> <p>Correct Permanent and present address</p>	<p>Any one of the documents other than mandatory.</p> <ol style="list-style-type: none"> I. Current valid Passport II. Income Tax PAN card (Mandatory) III. Voter's identity card IV. valid Driving licence V. Aadhar Card or letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number; VI. identity card (subject to the satisfaction of the Company). VII. any other officially valid document like job card issued by NREGA duly signed by an officer of the State Government <p>If Simplified Procedures are applied for verifying the identity of the individual 'low risk' customers, the following documents shall be deemed to be OVD:</p> <ol style="list-style-type: none"> 1. identity card with applicant's photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; 2. Letter issued by a Gazetted officer, with a duly attested photograph of the person.
		<p>Correct Permanent and present address</p>	<ol style="list-style-type: none"> I. Telephone bill II. Bank account statement III. letter from any recognized public authority IV. Electricity bill V. Ration card VI. Letter from employer (subject to satisfaction of the bank) VII. Passport <p>Additionally following OVDs (Officially Valid Documents) are acceptable for low risk customers for proof of</p>

			<p>address in case the above documents are not available:-</p> <p>a) Utility Bill which is not more than 2 months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill)</p> <p>b) Property or Municipal Tax Receipt</p> <p>c) Bank Account or Post Office savings bank account statement</p> <p>d) Pension or family pension orders (PPOs) issued to retired employees by Govt Departments or PSUs if they contain the address</p> <p>e) Letter of allotment of accommodation from employer issued by State or Central Govt departments, statutory or regulatory bodies, PSUs, scheduled commercial banks, FIs and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and</p> <p>f) Documents issued by Govt. departments off foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.</p> <p>* Not more than 3 months old</p>
			A copy of the marriage certificate or Gazette notification, in case of change in name
2	Accounts of partnership firms	<ul style="list-style-type: none"> ✓ Legal name, ✓ Address ✓ Names of all partners and their addresses ✓ Telephone numbers of the firm and partners 	<ul style="list-style-type: none"> (i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners

			(vi) Names & Address of the Partners / Authorised Signatories and Recent Passport Photographs duly self-attested.
3	Accounts of Proprietary Concerns	<ul style="list-style-type: none"> ➤ Legal name ➤ Address ➤ Activity ➤ Names of the Proprietor and his / her address ➤ Telephone numbers of the firm and Proprietor 	<p>Any two of the following documents in the name of the Proprietary Concern:</p> <p>i) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate / licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.</p> <p>ii) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.</p> <p>iii) The 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.</p> <p>iv) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.</p>
4	Accounts of Companies	<ul style="list-style-type: none"> ◆ Name of the company ◆ Principal place of business ◆ Mailing address of the company ◆ Telephone/Fax Number. 	<p>(i) Certificate of incorporation and Memorandum & Articles of Association;</p> <p>(ii) Certificate of Commencement of Business (in case of Public Ltd Co.);</p> <p>(iii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;</p> <p>(iv) Power of Attorney granted to its managers, officers or employees to transact business on its behalf;</p> <p>(v) Copy of PAN allotment letter;</p> <p>(vi) Copy of the telephone bill</p>
5	Accounts of trusts & foundations	<ul style="list-style-type: none"> ✚ Names of trustees, settlers, 	<p>(i) Certificate of registration, if registered</p> <p>(ii) Power of Attorney granted to transact business on its behalf;</p>

		beneficiaries and signatories;  Names and addresses of the founder, the managers/directors and the beneficiaries;  Telephone/fax numbers	(iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses; (iv) Resolution of the managing body of the foundation / association; (v) Telephone bill; (vi) Names & Addresses and Recent Passport Photograph of the Trustees/Managing Committee Members/Authorised signatories duly self-attested.
--	--	--	--

Notes:

1. For customers / clients who are Legal Person (who is not a natural person), the Beneficial Owner(s) shall be identified and all reasonable steps in terms of Client Acceptance Policy and CDD measure undertaken to verify his/her identity shall be undertaken.
2. The customers shall not be required to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address.
3. The customers shall not be required to furnish separate proof of address for permanent and current addresses, if these are not 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.
4. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as acknowledgment of receipt of letter, cheque books, ATM cards, telephonic conversation, visits to the place, or the like.
5. In case it is observed that the address mentioned as per 'proof of address' has undergone a change, it shall be ensured that fresh proof of address is obtained within a period of six months.
6. In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company will have the discretion to accept only one of those documents as activity proof. In such cases, the Company, will undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.
7. It is also clarified here that the list of registering authorities indicated in column 1 is only illustrative and therefore includes license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute, as one of the documents to prove the activity of the proprietary concern.
8. 'Officially valid document' is defined to mean the passport, the driving license, the Permanent Account Number card, the Voter's Identity Card issued by the Election Commission of India, Letter issued by the Unique Identification Authority of India containing details of name, address or any other document as may be required by the Company.
9. Simplified procedure as laid down in KYC Direction 2016 may be applied for small accounts

ANNEXURE – III

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

Identity of client

- ⇒ False identification documents
- ⇒ Identification documents which could not be verified within reasonable time
- ⇒ Accounts opened with names very close to other established business entities
- ⇒ Doubt over the real beneficiary of the customer

Background of client

- ⇒ Suspicious background or links with known criminals

Activity in accounts

- ⇒ Unusual activity compared with past transactions

Nature of transactions

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

Value of transactions

- ⇒ Value inconsistent with the client's apparent financial standing

B. Illustrative list of Suspicious Transactions

- ⇒ Reluctant to part with information, data and documents
- ⇒ Submission of false documents, purpose of loan and detail of accounts
- ⇒ Reluctance to furnish details of source of funds of initial contribution
- ⇒ Reluctance to meet in person, representing through power of attorney
- ⇒ Approaching a distant branch away from own address
- ⇒ Maintaining multiple accounts without explanation
- ⇒ Payment of initial contribution through unrelated third party account
- ⇒ Suggesting dubious means for sanction of loan
- ⇒ Where transactions do not make economic sense
- ⇒ Where doubt about Beneficial Ownership
- ⇒ Encashment of loan through a fictitious bank account
- ⇒ Sale consideration quoted higher or lower than prevailing area prices
- ⇒ Request for payment in favor of third party with no relation to transaction
- ⇒ Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent
- ⇒ Frequent request for change of address
- ⇒ Overpayment of installments with a request to refund the overpaid amount
- ⇒ Approvals/sanctions from authorities are proved to be fake
- ⇒ Overpayment of installments with a request to refund the overpaid amount