KYC & AML POLICY

Approved by the Board of Directors on April 28, 2026

1. Background

Five-Star Business Finance Limited (Five Star or the company) is a public limited company incorporated under Companies Act, 1956 and registered with the Reserve Bank of India. The Company is engaged in business of lending to individuals and non-individuals in the unorganized sector (secured by property as collaterals) towards starting small business units, to develop the existing business units/self-employed and meeting other personal expenses / financial needs. The loans would be provided basis the assessment of the household cash flows and against the collateral of their properties. The collateral is obtained by deposit of title deeds and registration of the same with Sub-Registrar office.

Reserve Bank of India 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. 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.

2. Objective:

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandates making reasonable efforts to determine the true 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. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

The policy seeks to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, the Company shall adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

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

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

This Policy will be applicable to all branches/offices of FIVESTAR.

3. Definition of a Customer

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

4. Customer Acceptance Policy (CAP)

The company shall follow the following norms while accepting and dealing with its customers.

a. The customer profile contains information relating to 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. However, while preparing customer profile the Company will 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 will not be divulged for cross selling or any other purpose.
b. The adoption of customer acceptance policy and its implementation should not be too restrictive and which result in denial of financial services to the general public, especially those, who are financially or socially disadvantaged. While carrying out due diligence, the company will ensure that the procedure adopted does not result in denial of services to any genuine customers.
c. The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the account holder is not known, the Company shall file suspicious Transaction Reporting (STR).
d. The Company shall not pursue the customer due diligence (CDD) if it is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the customer due diligence (CDD) process will tip-off the customer and instead the company shall file an Suspicious Transaction Reporting (STR).

The company shall ensure that:

a) No account is opened in fictitious / benami name or where the company is unable to do customer due diligence either on account of non-cooperation of the customer or non- reliability of the documents/ information given by customer
b) System is in place to check the identify of customer doesn't match with any person / entity, whose name appears in the sanctions of RBI.
c) Filing an STR is considered, if necessary when it is unable to comply with the relevant CDD measures in relation to the customer.
d) Additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer.

5. Risk Management

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing customer profile the Company will 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 will not be divulged for cross selling or any other purpose.

Risk categorization

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The risk categorization can be done based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc. An indicative categorization for the guidance of businesses is provided in Enclosure I.

Where businesses belienve that a particular customer falling under a category mentioned below is in his judgement falling in a different category, he may categories the customer so, so long as appropriate justification is provided in the customer file.

6. Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship. An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

a. verify the identity of any Person transacting with the Company to the extent reasonable and practicable.
b. Customers identity is also verified and validated by including all the resident family members into the application as co-applicants. Customer identification process is also a risk mitigation process embedded into.
c. maintain records of the information used to verify a customer's identity, including name, address and other identifying information and
d. Consult lists of known or suspected terrorists or terrorist organizations provided to the Company by any applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.

CIP will be undertaken on the commencement of a loan account opening for a customer. The company shall not take any introduction for opening an account.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

The company will not rely on customer due diligence done by a third party.

7. Customer Due Diligence (CDD) requirements

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. The Company shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers

and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

a. Identification

1) The Company shall be following from the individual while establishing account based relationship
   - A certified copy of any Officially Valid Document (OVD) listed in Enclosure 3 containing details of his identity and address.
   - The company may go for offline verification mode for Aadhaar, as per extant rules and regulations. The company may avail services of Business Correspondent (BC) for the same. However, the same will be in line with the RBI Master Circular on KYC guidelines.
   - Alternatively the verification through "Digital KYC" – introduced by RBI in 2016 and with subsequent amendments to the Master Directions 2016, the customer identity can be verified through capturing a live photo of the customer and officially valid document where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is taken by the authorised officer of the RE as per the provisions contained in the master circular .
   - If a customer submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, the Company may retrieve the KYC records online from the CKYCR using the KYC identifier and the customer shall not be required to submit the KYC records unless
     - there is a change in the information of the customer as existing in the records of CKYCR.
     - the current address of the customer is required to be verified.
     - the company 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 customer.
     - the validity period of documents downloaded from CKYCR has lapsed.
   - PAN or Form 60
   - If the account based relationship is established without customer submitting PAN/Form 60, then the customer shall submit the same within six months from the date of commencement of relationship. If the customer fails to submit the same, then no credit shall be allowed in such accounts. The company shall inform the customer above this provision at the time of opening of accounts.
   - One recent photograph
   - If the OVD listed in Enclosure 3 towards address proof doesn't have current address, then the company shall collect the following as proof of address:
     - Utility bill not more than 2 months old (i.e. electricity, telephone, post-paid mobile phone, piped gas, water bill)
     - Property or municipal tax receipt
     - Pension or family pension payment orders issued to retired employees by Government departments or PSU
     - Letter of allotment of accommodation from employer issued by state government or central government departments, statutory or regulatory bodies, PSU, scheduled commercial banks, financial institutions and listed entities

       In the above-mentioned instance, the company will collect OVD with current address within a period of 3 months of submitting the above documents.

2) For proprietary concerns, the company will collect documents from the list given in enclosure- 3 and only where the company is satisfied that it is not possible for the customer

to furnish two such documents, the company will have the discretion to accept only one of those documents as activity proof. In such a situation, the company will record the appropriate reason for accepting one document as activity proof.

3) For any corporates or other legal entities, the company will collect documents from the list given in enclosure-2 & 3

4) If an existing KYC compliant customer desires to open another account, there is no need for submission of fresh proof of identity and/or proof of address for the purpose. However, if there is a change in the residential address of the customer, a self-declaration and new residential address proofs are taken before opening of the new account.

b. Verification

The Company as a part of the credit policy will document and implement appropriate risk- based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. The acceptable methods of verification of customer identity may include verification through documents and/or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks thereof.

1. *Verification through documents:*

   These documents may include but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in enclosure-2 & 3 to this policy. The company representative shall compare the certified copy of OVD document collected with the original and record the same on the copy.

2. *Verification through non-documentary methods:*

   These methods may include, but are not limited to:

   1. Contacting or visiting a customer:
   2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source:
   3. Checking references with other financial institutions: or
   4. Obtaining a financial statement.
   5. If a full KYC verification is done by a branch / office and is not due for a periodic updation for an account: then it is valid for a transfer to another branch/office or the company.
   6. As included in the enclosure 4, verification can be done thru Digital KYC - the customer identity can be verified through capturing a live photo of the customer and officially valid document where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is taken by the authorised officer of the RE as per the provisions contained in the master circular.

c. Resolution of Discrepancies

The company will implement procedures to resolve information discrepancies and, if not resolved, to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence.

8. Periodic updation of KYC records (Ongoing Due Diligence):

Full KYC exercise (periodic updation) will be done at a periodicity not less than once in ten years in case of low risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high risk category customers. At the time of revalidation, the company shall obtain a fresh certified copy of

1. PAN or Form 60.
2. Any OVD document as detailed in Enclosure 3.
3. Digital KYC as per the provisions contained in the KYC Master Circular
4. However, in case of low risk category and no change in status with respect to their identities and addresses, then a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they can forward a certified copy of proof of address by mail/post, etc.
5. In case of any customer other than individual, the documents as detailed in Enclosure 3 shall be obtained
6. This exercise would apply from the date of opening of account/last verification of KYC.

9. Money Laundering and Terrorist Funding:

The Company shall ensure to carry out a periodic Money laundering (ML) and Terrorist Financing (TF) risk assessment exercise to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk for clients, countries or geographic areas, products services, transactions or delivery channels etc. The risk assessment will be done by taking the cognisance of overall sector specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.

Five Star shall apply Risk based approach for mitigation and management of the identified risk through Board approved policies, controls and procedures. The same will be reviewed by RMC on an annual basis.

10. Enhanced due Diligence

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing credit policies of the Company in respect of its businesses ensure that the Company is not transacting with such high risk customers. The Company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. Each business process shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence. Enhanced Due Diligence shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

i. Customers requesting for frequent change of address/contact details
ii. Sudden change in the loan account activity of the customers
iii. Frequent closure and opening of loan accounts by the customers
iv. Accounts of Politically Exposed Persons (PEP)

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorisation of risk, updating of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

The Company will not do any transactions with non-face-to-face customers.

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

The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

In a scenario wherein an account has to be opened for a PEP after a detailed assessment of the source of funds, identity of the PEP, Details on his activities carried out by him and his family members; it shall be approved by COO / CCO, HD – Operations and MD/CEO prior to opening of an account. If an existing customer subsequently becomes a PEP, then approvals has to be taken from the above mentioned designated individuals in order to continue the relationship. Such account would be tagged as "High Risk Customers" and all the process and procedures, not limited to CDD measures, including enhanced monitoring would be applicable.

The Company shall not on rely on third party due diligence or open accounts through professional intermediaries.

11. Record Retention

- The company shall maintain all records of transaction between company and the customer for at least 5 years from the date of transaction.
- The company shall preserve identification / address documents of customer that includes updated records of the identification data, account files, business correspondence and results of any analysis undertaken for a period of 5 years after the business relationship is ended
- The company shall maintain a record of transactions as prescribed in Prevention of money laundering act. The details are given below:
    1. Transactions for which records need to be maintained:
        i. All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
        ii. All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.

iii. 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.
iv. All suspicious transactions whether or not made in cash.

2. Information to be preserved:
   i. The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

- The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

12. Reporting

The company shall have a system of internal reporting of cash transactions greater than Rs.10 lakhs (whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other and where such series of transactions take place within a month) ,suspicious transactions and counterfeit transactions , whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bona fide purpose; or
d. give rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
e. Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Further, the Principal officer shall furnish information of the above mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the principal officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.10 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time

13. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High-risk accounts have to be subjected to intensified monitoring.

The Company shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

14. CIP Notice

The Company shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

15. Existing Customer

The requirements of the earlier sections are not applicable to existing customers, unless specifically mentioned in the policy or notified by Government / regulators. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

16. Customer Education

The Company may regularly educate the customer of the objectives of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC through training programmes/e-mail.

17. Applicability to branches and subsidiaries outside India

The above guidelines shall also apply to the branches.

18. Appointment of designated Director or Principal Officer:

The Board may nominate Chairman & Managing Director or Whole Time Director to act as designated director who will be responsible for ensuring overall compliance as required under PMLA Act and the Rules. Principal Officer shall be responsible for furnishing of information to FIU-IND.

19. Hiring of Employees and Employee training

a. The company shall ensure that adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment / hiring process shall be put in place.

b. The company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

c. On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

20. Illustrative list of activities which would be construed as suspicious transactions

Activities which are not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits shall be construed as suspicious transactions.

Any attempt to avoid reporting / record-keeping requirements / provides insufficient / suspicious information:

1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
2. Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
3. An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
4. Certain Employees of the Company arousing suspicion:
5. An employee whose lavish lifestyle cannot be supported by his or her salary.
6. Negligence of employees / wilful blindness is reported repeatedly.
7. Some examples of suspicious activities/transactions to be monitored by the operating staff:
8. Multiple accounts under the same name
9. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc;
10. There are reasonable doubts over the real beneficiary of the loan
11. Frequent requests for change of address

21. Compliance of KYC Policy

i. For the purpose of KYC compliance, the Managing Director, CEO, CRO, COO, CCO and Head Operations are constituted as "Senior Management".

ii. For day to day operations COO, Business Head, CCO and Head Operations would ensure that the KYC policies and procedures are implemented effectively and efficiently.

iii. The External Internal Auditor, as appointed time to time by the company, would verify the adherence of the KYC policy during the normal course of conducting their auditing activities and would bring any deviation/discrepancy, if any, to the Audit Committee

iv. Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function also provides an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements. Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard is put up before the Audit Committee of the Board on quarterly intervals.

v. On a quarterly basis, the audit points, if any, and compliance would be presented to the Audit Committee.

vi. The decision-making function of the determining compliance with the KYC policy/norms will not be outsourced by the company

22. Central KYC Registry (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for individuals with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

1. Whenever RE receives an Additional or Updated information from an Existing Customer, the same shall be informed to CKYCR within seven days or within such period as may be notified by the central Government.

2. Once CKYCR informs RE regarding an update in the KYC of an existing customer, the RE shall retrieve the updated information from CKYCR and shall update the same in their records.

3. While Establishing an Account based Relationship or while updation /periodic updation of KYC, the RE shall seek for KYC Identifier from the customer or retrieve the KYC Identifier from CKYCR. The RE shall proceed to obtain KYC from online records and not require the customer to submit the same.

Enclosure-1

Indicative List for risk categorisation Medium & High Risk Category

Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples of medium risk category customers are:

1. High Net worth Individuals (Having defined as income of more than INR 1 Crore pm)
2. Trust, charities, NGO's and Organization receiving donations
3. Companies having close family shareholding or beneficial ownership
4. Firms with 'sleeping partners'
5. If all the customers, part of a proposal, stays outside of India

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
2. Non face-to-face customers
3. Those with dubious reputation as per public information available

Low Risk Category

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile and not covered in any of the above two categories, shall be categorised as low risk.
Since most of the Company's customers are based out on India and are serviced by the Company thru its own branches and employees and transacts only in INR with the Company, they would be classified as low risk .

Illustrative examples are:

1. Salaried employees whose salary structure is well-defined
2. People belonging to lower economic strata of the society whose accounts show small balances

and low turnover

Enclosure-2

Customer Identification Requirements Trust Accounts

The company shall collect following for opening a Trust account:

1. Registration certificate, if registered
2. Trust deed
3. An identification document in respect of the person holding an attorney to transact on its behalf in line with KYC policy

In the case of any application from 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 in doubt of the persons behind the customer, the Company may 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. Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms

For opening an account of a company, we shall collect certified copies of each of the following documents:

a) Certificate of incorporation
b) Memorandum and Articles of association
c) Board resolution and Power of attorney granted to its managers, officers or employees to transact on its behalf
d) An identification document in respect of the managers / officers /employees / person holding an attorney to transact on its behalf in line with KYC policy

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the 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 exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership

Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:

I. "Controlling ownership interest" means ownership of or entitlement to more than twenty five percent of shares or capital or profits of the company;
II. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements;

(a) where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

(b) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(c) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(d) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

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

Enclosure-3

KYC Documents for Identification and verification

List of documents required for CIP (Customer Identification Procedure):

	To submit Certified copy of the following document
Resident Individual	Mandatory Document: PAN/Form 60 plus any one OVD as mentioned below 1. Passport 2. Voter's identity Card issued by Election Commission. 3. Driving License 4. Job card issued by NREGA duly signed by an officer of the State Govt. 5. The letter issued by the national population register containing details of name and address. 6. Digital KYC – the customer identity can be verified through capturing a live photo of the customer. 7. Proof of Possession of Aadhar number with Aadhaar number stricken.
Partnership Firms	1. Registration certificate, if registered 2. Partnership deed 3. An officially valid document in respect of the person holding an attorney to transact on its behalf.
Proprietor Concern	The company shall collect kyc documents of proprietor in line with the policy. With respect to proprietary concern, the company shall collect any two of the following documents as a proof of business /activity in the name of proprietary firm: 1. Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), 2. certificate/licence issued by the Municipal authorities under Shops & Establishments Act 3. sales and income tax returns, 4. CST/VAT / GST certificate (provisional /final) 5. Registration certificate including Udyam Registration Certificate (URC) issued by the Government 6. Certificate/registration document issued by Sales Tax/Service Tax / Professional Tax authorities, 7. Importer Exporter Code (IEC) issued to proprietary concern by the office of DGFT /Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. 8. 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. 9. Utility bills such as electricity, water and landline telephone bills.

Enclosure – 4

Relevant Process of V-CIP (Video based Customer Identification Process) as per Amendment to Master Direction (MD) on KYC, 10th May 2021.

The process of V-CIP has been specified in Section 18 in terms of which, REs may undertake live V-CIP, to be carried out by an official of the RE, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

a. The official of the RE performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information. REs other than banks: can only carry out Offline Verification of Aadhaar for identification.
b. RE shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.
c. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India
d. The official of the RE shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.
e. The official of the RE shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.
f. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.
g. RE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. RE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.
h. To ensure security, robustness and end to end encryption, the REs shall carry out software and security audit and validation of the V-CIP application before rolling it out.
i. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.
j. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.
k. REs are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.
l. RE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.