KYC & AML POLICY -ARYADHAN FINANCIAL SOLUTIONS PVT LTD

KNOW YOUR CUSTOMER

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.

This Policy requires the Company and each Employee to:

- Protect the Company from being used for money laundering or funding terrorist activities
- Comply with the letter and the spirit of applicable AML/CTF Laws, and the Company's AML Program and procedures
- Be alert to and escalate suspicious activity
- Cooperate with AML-related law enforcement and regulatory agencies to the extent permitted under applicable laws.

Accordingly, in compliance with the guidelines issued by **RBI- Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on May 04, 2023)** (Master Direction DBR.AML.BC.No.81/14.01.001/2015-16), the following KYC & AML policy of the Company is approved by the Board of Directors ofthe Company. This policy is applicable to all categories of products and services offered by the Company.

OBJECTIVE

Objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionallyby criminal elements for money laundering activities. The guidelines also mandate 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 isto enable the Company to have positive identification of its customers.

KEY ELEMENTS OF POLICY

The Company is hereunder framing its KYC Policy incorporating the following four key elements:

- Customer Acceptance Policy (CAP)
- Risk management
- Customer Identification Procedures (CIP)
- Monitoring of Transactions

CUSTOMER ACCEPTANCE POLICY

The Company shall follow the following norms while accepting and dealing with its customers:

Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his/her clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk. The illustrative list of such risk categorisation is provided in annexure – I.
The customer profile contains information relating to customer's identity, social/financial status,

nature of business activity, information about his/her 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.

The intent of the Policy is not to result in denial of financial services to general public, especially to 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.

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) as per details provided in Annexure IV

CUSTOMER IDENTIFICATION PROCEDURE

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 Customer Identification Procedure (CIP) to be carried out at different stages i.e. while establishing a business relationship; creating an account based relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. 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:

- Verify the identity of any Person transacting with the Company to the extent reasonable and practicable
- Maintain records of the information used to verify a customer's identity, including name, address and other identifying information and
- 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.

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.

REQUIRED KYC DUE DILIGENCE FOR ALL CUSTOMERS

The Company shall take reasonable measures to ascertain and verify the true identity of allcustomers who transact with the Company. Each business process 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:

IDENTIFICATION

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have abetter approach to risk profiling of customers.

Each business process shall implement procedures to obtain from each Customer, prior to transacting, the following information as may be relevant, to that business:

1. Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;
2. For individuals - age / date of birth; For a person other than individual (such ascorporation, partnership or trust) - date of incorporation;
3. Address including the documentary proof thereof;
    I. For an individual, a residential or business street address;
    II. For a Person other than an individual (such as a corporation, partnership, ortrust), the principal place of business, local office, or other physical location;
4. Telephone/Fax number/E-mail ID;
5. Identification number:
    I. A taxpayer identification number; passport number and country of issuance;letter issued by Unique Identification Authority of India containing AADHAAR number; alien identification card number; or number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard. When opening an account for a person (other than an individual) that does not have an identification number,the business process must request alternative government issued documentation certifying the existence of the business or enterprise;
    II. For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but each business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before disbursal of loan.

Fresh photographs will be obtained from minor customer on becoming major whereverapplicable.

Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required. Biometric based e-KYC authentication can be done by company officials whenever required. The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.
The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as annexure III to this policy. These are appropriately covered in the credit policies of the respective businesses andcommunicated to the credit approving authorities.

For proprietary concerns, the company will collect any two documents from the list given in annexure III 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 recordthe appropriate reason for accepting one document as activity proof.

If an existing KYC compliant customer desires to open another account, there is no needfor submission of fresh proof of identity and/or proof of address for the purpose.

VERIFICATION

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

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 productsoffered by the Company as provided in annexure - II to this policy. These are appropriately covered in the credit policies of the respective businesses. The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as annexure II to this policy. These should be appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

Verification through non-documentary methods:

These methods may include, but are not limited to:

- Contacting or visiting a customer;
- 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;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

Additional verification procedures:

If applicable, the business process verification procedures should address situationswhere:

- A person is unable to present an unexpired government-issued identificationdocument that bears a photograph or similar safeguard;
- The business process associate is not familiar with the documents presented;
- The Account is opened without obtaining documents;
- Where the business process is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customerthrough documents; and
- If the business process cannot verify the identity of a customer that is other than an individual,

it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

Where a low-risk category customer expresses inability to complete the documentation requirements on account of any reason that the Company considers tobe genuine, and where it is essential not to interrupt the normal conduct of business, the Company may complete the verification of identity within a period of six months from the date of establishment of the relationship.

RESOLUTION OF DISCREPENCIES

Each business process shall document and implement procedures to resolve information discrepancies and 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. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

REPORTING

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and 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 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) gives rise to a reasonable ground of suspicion that it may involve financing ofthe 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 Compliance officer shall furnish information of the above-mentioned transactions to the Head Risk & Credit of the company at the prescribed address inthe formats prescribed in this regard including the electronic filing of reports.

Provided that where the Head Risk & Credit, 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, shall furnish information in respect of such transactions to the Director within the prescribed time.

REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA: All transactions of cash and suspicious as required under PML Act 2002 shall be reported to Financial Intelligence Unit (FIU) from time to time. The Principal Officer shall ensure that such reporting system is in place and shall monitor receipt of the reports.

RECORD RETENTION

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

A) Transactions for which records need to be maintained:

1. All cash transactions of the value of more than Rs.10 lakhs or its equivalentin foreign currency.
2. 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 monthand the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.
3. All cash transactions where forged or counterfeit currency notes orbank notes have been used as genuine and where any forgery of a valuable security has taken place.
4. All suspicious transactions whether or not made in cash.

B) Information to be preserved:

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.

C) Periodicity of retention:

The following records shall be retained for a minimum period of five years after the related account is closed:

1. The customer identification information and residence identification information including the documentary evidence thereof
2. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least five (5) years after such record was created.

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

CUSTOMER CIP NOTICE

Each business process 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.

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 various 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 processshall 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, that 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:

- Customers requesting for frequent change of address/contact details
- Sudden change in the loan account activity of the customers
- Frequent closure and opening of loan accounts by the customers

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

RELIANCE ON THIRD PARTY DUE DILIGENCE

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party;subject to the conditions that

- the Company immediately obtains necessary information of such client due diligence carried out by the third party;
- the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record- keeping requirements in line with the requirements and obligations under the Act;
- the third party is not based in a country or jurisdiction assessed as high risk; and
- the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

RISK CATEGORIZATION

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

The Company shall have a system in place for periodical updation of customer identification data

after the account is opened. Full KYC exercise 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. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC. Documents as specified will be taken/reviewed at the time of periodic updation.

Low risk category customers need not submit fresh proofs of identity and address at the time of periodic updation, in case of no change in status with respect to their identities and addresses and 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. Fresh photographs will be obtained from minor customer on becoming major. Fresh CDD & KYC, if required may be carried out.

In case of Legal entities, if there is no change in KYC then a self-declaration will suffice but in case if change in KYC, the Company shall review the documents sought at the time of opening of account and obtain fresh certified copies through the registered email id of the legal entity.

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization.An indicative categorization for the guidance of businesses is provided in Annexure - I. Each business process adopts the risk categorization in their respective credit policies subject to confirmation by compliance based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, 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. etc., Where businesses believe that a particular customer falling under a category mentioned below is inhis judgement falling in a different category, he may categorize the customer so, so long as appropriate justification is provided in the customer file. For completely secured retail finance products, such categorization may be waived.

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.

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 and comment on the lapses observed in this regard.

The compliance in this regard is put up before the Board on quarterly intervals.

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 transactionsthat fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. The different 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 throwalerts when the transactions are inconsistent with risk categorization and updated profile of customers.

SECRECY OBLIGATION AND SHARING OF INFORMATION

The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the customer and itself. No details shall be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

SHARING OF KYC INFORMATION WITH CKYCR

Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, RBI KYC Direction issued from time to time, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. CERSAI guidelines for uploading will be applicable. The Company shall ensure that the KYC identifier is communicated to the individual/LE as the case may be.

CUSTOMER EDUCATION AND EMPLOYEE TRAINING

The Company may prepare specific literature/ pamphlets etc. so as to 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 various training programmes and e-mails.

APPLICABILITY TO BRANCHES AND SUBSIDARIES

The above guidelines shall also apply to the branches and subsidiaries of the Company in and outside India

APPOINTMENT OF DESIGNATED DIRECTOR/ PRINCIPAL OFFICER

Mr. Inderjeet Singh, General Manager of the Company is responsible for ensuring overall compliance as required under PMLA Act and the Rules. Head Risk & Credit is designated as Principal Officer who shall be responsible for furnishing of information.

Annexure I

Aryadhan KYC Norms

Documents	Applicability	Self-attestation	Original Seen & Verified
KYC -Pan Card	Directors/Proprietor/Partners/Individual borrower	Required, only signature, no stamp	Required (Name & Employee Code mandatory)
Land Record	Individual	Required, only signature, no stamp	Required (Name & Employee Code mandatory)
KYC -Aadhar Card /Voter Id/Bank Pass book/Electricity bill/Driving license	Directors/Proprietor/Partners/Individual borrower	Required, only signature, no stamp	Required (Name & Employee Code mandatory)
Pan Card of the firm (in case of non-individual cases)	Proprietorship Firm/Partnership firm/Pvt Ltd/FPO/AOP	Required with stamp and signature of Director/Partner/Proprietor	Required (Name & Employee Code mandatory)
Address Proof of the firm-GST certificate/Udhyam Registration Certificate/Bank passbook/Electricity bill	Proprietorship Firm/Partnership firm/Pvt Ltd/FPO/AOP	Required with stamp and signature of Director/Partner/Proprietor	Required (Name & Employee Code mandatory)
MoA & AoA, Certificate of Incorporation	Private limited (Mandator document)/FPO	Required with stamp and signature of Director (1st & Last Page)	Required (Name & Employee Code mandatory)
Partnership Deed	Partnership Firm (Mandatory Document)	Required with stamp and signature of Partner (1st & Last Page)	Required (Name & Employee Code mandatory)
Audit report & Financials (Last two financial years)	Proprietorship Firm/Partnership firm/Pvt Ltd/FPO/AOP	Required with stamp and signature of Director/Partner/Proprietor (1st page, Last page and middle page)	Not required
*UDIN no. Mandatory			
Provisional financials CA certified or Provisional financials self-certified	Proprietorship Firm/Partnership firm/Pvt Ltd	Required with stamp and signature of Director/Partner/Proprietor	Not required
Bank Statement (last 6 months) Pdf format	Proprietorship Firm/Partnership firm/Pvt Ltd	Required with stamp and signature of Director/Partner/Proprietor	Not required

		(1st page, Last page and middle page)	
GST returns of last 4 quarters -cases >1.5 Cr and up to 3 Cr	Proprietorship Firm/Partnership firm/Pvt Ltd	Required with stamp and signature of Director/Partner/Proprietor	Not required
Note: Additional documents as per requirement: for e.g., Dual name declaration, vernacular declaration, Security cheques, Self-declaration of Proprietor, Partnership Authority letter, Board Resolution			

***Wherever verification is being done OTP based OSV would not be required.**
***Wherever physical verification is being done OSV would be required.**