Avanti Microfinance Private Limited

KYC / AML Policy

This document was:

Version	Drafted by	Reviewed by	Board approval and adoption date
Version 1	<>	<>	October 30, 2017
Version 2	Mr. Nagaraj Subrahmanya, Director	Mr. Manish Thakkar, Director	December 16, 2024
Version 3	Mr. Nagaraj Subrahmanya, Director	Mr. Manish Thakkar, Director	August 01, 2025

Document Classification**: Public**

Table of Contents

1. Introduction

In the current economic scenario, it is imperative that appropriate measures are taken to prevent intentional/unintentional usage of channels by criminal elements for money laundering or terrorist financing activities. Avanti Microfinance Private Limited (hereinafter referred to as "Company") will consistently work towards developing robust Know Your Customer (KYC) principles and Anti-Money Laundering (AML) standards to know/ understand its customers and their financial dealings and manage risks arising out of such financial dealings prudently. RBI vide its master circular has advised to put in place a Board approved AML/KYC policy framework, which shall document the underlying principles for customer acceptance, customer identification, transaction monitoring and risk management.

2. Objectives of the Policy

The policy aims to develop a diligent and compliance sensitive culture in the Company through a focused approach on customer acceptance and identification procedures.

The key objectives of the policy are as under:

(i) Prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities, through the various channels, products and services it offers;

(ii) Define a mechanism for risk categorisation of customers at the time of account opening and transaction monitoring measures commensurate with the risk categorisation of the customers;

(iii) Enable the Company to know / understand its customers and their financial dealings better and manage its risks in a prudent manner;

(iv) Allocate responsibility for effective implementation of policy and ensure adequate training on KYC procedures is provided to the concerned staff;

(v) Develop a comprehensive AML/ Combating Financing of Terrorism (CFT) programme in line with the regulatory requirements covering systems and controls, training of staff and management oversight and ensure its effective implementation.

3. Applicability

This policy shall be applicable to all verticals / products of the Company whether existing or rolled out in future. It may be noted that KYC – AML policy as stated in this document shall prevail over anything else contained in any other document / process / circular / letter / instruction in this regard (KYC-AML). This policy shall be applicable to all verticals/products of the Company whether existing or rolled out in future.

4. Governance Structure

The Company shall have a robust governance structure to monitor compliance with KYC / AML / CFT guidelines across all functions / business units of the Company. The Risk Management Committee ("RMC"), administered and complied at the consolidated group level by Avanti Finance Private Limited, the holding company will, inter alia, oversee the implementation of the AML/ KYC framework. There shall be a designated director who shall be different from the Principal Officer.

The Company has a senior management officer to be designated as the Principal Officer who will facilitate and monitor compliance with regulatory guidelines with respect to customer acceptance, customer identification, and transaction monitoring and risk management. The Principal Officer will ensure that the cash and suspicious transactions reporting are done in a timely manner and accurately to the regulator. He will also ensure appropriate dissemination of regulatory updates, pertaining to KYC/ AML/ CFT and guide these business units on compliance. For the purposes of this Policy, the Senior Management in the Company shall consist of: (a) the Chief Operating Officer, and (b) the Chief Risk Officer, of the holding company i.e. Avanti Finance Private Limited who will be responsible for effective implementation of this Policy and the procedures laid in the Policy.

At branch level/ Centers / Mandi, the responsibility for ensuring compliance with KYC norms will rest with the Service Representative or staff of the Company.

5. Key Elements of the Policy

In line with the RBI guidelines, the KYC policy shall comprise of the following components:

5.1 Customer acceptance
5.2 Customer identifications
5.3 Transaction monitoring
5.4 Risk management.

5.1 Customer Acceptance

The Company's Customer Acceptance Policy (CAP) lays down the criteria for acceptance of customers.

A customer is any person who enters into any financial dealing or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity is acting.

The customers may approach the Company to avail of the products and services offered through branches, Consultants / agents or through digital channels such as mobile application and website. All these channels:

(i) Will accept customers only after verifying their identity;

(ii) Prohibit the opening of anonymous or fictitious/ benami accounts;

(iii) Ensure necessary checks before opening a new account so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.;

(iv) While opening the Company accounts for these customers, specifically in rural areas, the Company will use multiple sources such as e-KYC service of UIDAI, mobile application and tab to capture the KYC details of the customer along with the required KYC documents;

(v) Not to allow existing customers to continue or accept new customers if they are on the sanctions list as set out by RBI or any other lists prescribed by the relevant regulators;

(vi) Will check the risk perception of the customers based on the parameters defined by the Risk Management Committee from time to time. Parameters of risk

perception will be clearly defined in terms of the location of customer and his clients and mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into low, medium and high risk;

(vii) Will adhere to the documentation requirements and other information which is to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act 2002 as amended by PMLA 2009 and subsequent amendments, (hereinafter referred to as PMLA), rules framed there under, and guidelines issued from by regulators;

(viii) Will not to open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures, i.e. the Company is unable to verify the identity and / or obtain documents required as per the risk categorisation due to non- cooperation of the customer or unreliability of the data/information furnished;

(ix) Will ensure that the circumstances in which a customer is permitted to act on behalf of another person/entity is in conformity with the established law and practices, and the customer should be able to explain satisfactorily the reason / occasion why an account needs to be operated by a mandate holder or where an account may be opened by an intermediary in a fiduciary capacity;

(x) All the Customers would be classified under appropriate risk weights;

(xi) Open accounts for PEPs after clearance from Principal Officer and monitor operations in such accounts on an on-going basis. PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. They would be subjected to enhanced Customer Due Diligence (CDD) and such accounts would be permitted at least at a level higher than what is otherwise permitted to approve the account. Close relatives of PEP also would be treated at par with PEP;

(xii) All customer accounts deemed to be high risk to be opened with the specific approval of Principal Officer;

(xiii) Shall have in place suitable built-in safeguards to avoid harassment of the customer.

(xiv) if an existing customer with valid KYC, desires to open another account or avail any other product or service from the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

Further, the Company shall ensure that appropriate KYC procedures are duly applied to agents/field officer of LSPs, who are sourcing the customers.

The Company will develop appropriate systems for adoption of E-KYC procedure facilitated by the Unique Identification Authority of India (“UIDAI”). The customer details would be obtained as under:

(a) Release of information by UIDAI on customer consent through biometric verification;

(b) Printing e-Aadhaar letter based on the Aadhaar number provided by the customer.

Under the e-KYC procedure, the information containing demographic details and

photographs made available from UIDAI will be treated as OVD. The data of the individual comprising of name, age, gender, and photograph of the individual will be transferred electronically to the branches, Service representatives appointed by the Company post biometric authentication by the individual. The Company will then print the e-Aadhaar letter of the prospective customer directly from the UIDAI portal for KYC validation and documentation. If the prospective customer knows only his/her Aadhaar number, the Company may print the prospective customer's e-Aadhaar letter in the Company directly from the UIDAI portal; or adopt e-KYC procedure as aforementioned.

5.2 Risk Category and Customer Profile

The Company shall prepare a profile for each new customer based on risk categorization as mentioned in this policy. Company shall review risk categorization of customers on half yearly basis and the need for applying due diligence measures.

The Company will ensure adequate care for preparation of customer profile so as to seek only relevant information which is relevant to the customers risk category. In case the Company requires any other details, it should be sought separately only with the customer's consent. The Company understands that the details obtained from the customer are confidential and will ensure adequate care and security for the safekeeping of the data and shall not divulge the data for cross-selling or any other purpose.

Risk Category

Company will classify its customers based on the following principles and in accordance with the below mentioned risk categories (as may further be modified / supplemented by RBI from time to time), i.e., Low Risk; and Medium Risk / High Risk.

It is important to bear in mind that the adoption of the below categorization and its implementation should be viewed as guidance so that they do not become too restrictive and result in denial of Company's services to general public, especially to those, who are financially or socially disadvantaged.

Low Risk:

For the purpose of risk categorization, individuals (other than High Net Worth individuals) and entities whose identities can be easily identified, may be categorized as low risk. Illustrative examples of low risk customers could be:

(A) salaried employees whose salary structures are well defined;
(B) persons belonging to lower economic strata of the society whose accounts show nil or small balances / low turnover; and
(C) Government departments & Government owned companies, regulators and statutory bodies, etc.

In such cases, Company will obtain and verify only the basic set of documents as prescribed under law for the purpose of KYC.

Medium / High *Risk*:

Customers that are likely to pose a higher than average risk to the Company 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.

Company requires extensive due diligence for higher risk customers, especially those for whom the sources of funds are not clear.

Illustration of customers requiring higher due diligence may include:

(A) high net worth individuals;
(B) politically exposed persons (PEPs) of foreign origin;
(C) non-resident customers;
(D) Customers onboarded in non face-to-face mode through use of digital channels such as CKYCR, DigiLocker, offline Aadhaar, equivalent e-document etc
(E) trusts, charities, non-governmental organizations and entities receiving donations (whether domestic or from international sources);
(F) companies having close family shareholding or beneficial ownership; and
(G) those with dubious reputation as per public information available.

In addition, parameters of risk perception shall include:

5.3 Customer Identification Procedure

Company shall ensure adherence of Customer Identification Procedure as prescribed by the Reserve Bank of India from time to time. The Company would obtain the KYC documents whenever there is doubt about the authenticity/veracity or the adequacy of the previously obtained Customer identification data. If Aadhaar card is taken as KYC, Company would satisfy itself about current address by obtaining required proof. The Company also have the process of allotting Unique Customer Identification Code (UCIC) for easy identification of all the relationships of any Customer with the Company.

Information collected for the purpose of opening of 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 one credit information agency approved by RBI. Information sought from the Customer would be relevant to the perceived risk and would not be intrusive. The Beneficial Owner in the case of trust, partnership and Joint stock companies would be reckoned in pursuance of this policy.

5.4 Transaction Monitoring

Company would continue to maintain proper record of all cash transactions as may be prescribed under applicable law. The Company shall obtain copy of PAN of all the Customers for cash transaction of Rs 50,000 or more entered into with them. In case a Customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

Company would strive to have an understanding of the normal and reasonable activity of the Customer through personal visits and by observing the transactions and conduct of the account in order to identify transactions that fall outside the regular pattern of activity – unusual transactions.

For the simplicity of data capture, the following transactions would be considered as unusual transactions deserving special attention (in addition to those listed in Annexure 3):

(i) Repeated pre termination of loan accounts of size exceeding Rs.10 lacs;
(ii) Same Customer appearing in the Cash Transaction Report (CTR) more than 3 times during a span of 6 months;
(iii) Total cash received from a customer exceeding Rs 50 lacs in a financial year or Rs 25 lacs in a month.

Such accounts would be treated as Medium/High Risk Customers after review of the unusual transactions by the Principal Officer – PMLA.

Being an NBFC, Company is not empowered to seize any counterfeit currency like in the case of banks. However, the following incidents of counterfeit currency at the cash counters would be recorded and repeated occurrence would be reported:

(i) Bulk counterfeit currency of more than 10 pieces at a time;
(ii) Repeated event within a week from a collection executive or Customer.

All such transactions would be reported to and reviewed by Principal Officer – PMLA who would enquire into the matter and decide whether the transaction would qualify to be termed as a suspicious transaction. When it is believed that we no longer are satisfied that we know the true identity of the account holder, STR would be filed with FIU-IND. The Principal Officer - PMLA would file the Suspicious Transaction Report (STR) with the Director, Financial Intelligence Unit-India (FIU-IND) within 7 days of identifying them. After filing STR, transactions would be allowed to be continued in the account unhindered and the Customer would not be tipped in any manner.

All CTR/STR would be filed electronically or as per the norms stipulated by FIU-IND from time to time. The STR would be filed even for attempted transactions.

List of individuals and entities, approved by UN Security Council Committee and circulated by RBI would be updated and the list would be available at every office entrusted with the responsibility of customer acceptance and would be verified before opening an account. Financial Action Task Force (FATF) statements regarding countries with deficient AML/CFT would be verified and caution would be exercised with Customers who conduct business activities in these countries.

5.5 Risk Management

The Company shall develop appropriate procedures for customer acceptance, identification and monitoring. The Company will constantly strive to strengthen its KYC framework in order to mitigate following key risks which may arise due to inadequate KYC standards:

(a) Money laundering risks and risks of financing of terrorist activities
(b) Compliance risk
(c) Reputation risk
(d) Fraud risk
(e) Legal risk

The Board of the Company shall develop an effective AML / CFT programme through establishment of appropriate procedures and allocate responsibility to senior management for effective implementation of the policy and will cover aspects such as systems and controls, management oversight, segregation of duties, training staff and other related matters. A risk based approach will be adopted to address management and mitigation of various AML / CFT risks.

The Risk and Compliance Department of the holding company will conduct an assessment exercise of the above risks on an annual basis considering the Company's customer segment, nature, size, geographical presence, complexity of activities/structure, etc. The outcome of the exercise shall be put up to the Board of the Company.

Internal Auditors will conduct independent evaluation to assess the effectiveness of implementation of policies and procedures, including legal and regulatory requirements and further, will check and verify the application of KYC/AML procedures at the branches and for accounts routed through Consultants/ Agents and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Board on quarterly intervals.

5.6 Customer Education

Implementation of KYC procedures require the Company to demand certain information from customers which may be of personal nature, or which have hitherto never been called for. This can sometimes lead to questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for the Company to prepare specific literature / pamphlets / notices, etc. so as to educate the customer about the objective of the KYC programme. The front desk staff will be specially trained to handle such situations while dealing with customers.

5.7 Introduction of New Technologies, New Products, New business practices

The Company shall pay special attention to any money laundering threats that shall arise from new or developing technologies, products, business practices including internet transactions that might favour anonymity, and take measures, if need, to prevent their use in money laundering schemes.

Further, REs shall ensure to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies.

6. Periodical Review of Customer Identification Data

(i) Periodic updation means steps taken to ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI. Updation/periodic updation of the KYC can be undertaken at any Branch of the Company or through Company mobile/web application.

(ii) The Company will conduct revalidation of KYC, which will include confirming identity and address of the customer, assessment of risk profile of the customer based on the last updated KYC and seeking additional data, including the source of funds / wealth, if required, from the customer. Timeframe for such revalidation would be as under and would apply from the date of account opening/ last verification date of KYC.

Risk Categorization	**Periodicity (At least)**
High Risk Customers	Every two years
Medium Risk Customers	Every eight years
Low Risk Customers	Every ten years

(iii) Further, in case the validity of the CDD documents available with the Company has

expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

Subject to KYC guidelines (as notified by RBI from time to time):

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

(ii) For 'low risk' customers, certified copy of address proof will be obtained (through mail / post) only if there is a change in the address of the customer. Physical presence of the customer at the branch will not be insisted upon;

(iii) 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 verified within a period of two months;

(iv) Company may, at its option, obtain a copy of OVD or deemed OVD, as prescribed by RBI, or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation/periodic updation;

(v) In case of existing customers, the Company shall obtain the Permanent Account Number or equivalent e document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which the Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer

(vi) Acknowledgment will be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation/ periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/ periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer;

(vii) In case the customer does not comply with KYC requirements, the Company will either terminate the existing relationship or carry out necessary actions to temporarily cease the business relationship in accordance with the provisions of the RBI's Guidelines on "Know Your Customer" and Anti-Money Laundering Measures, as amended from time to time.

Provided that before terminating or temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, the Company shall provide appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide PAN or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with the Company gives in writing to the Company that he does not want to submit his PAN or Form No.60, the Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

7. Record Keeping

Section 12 of PMLA, 2002 requires that the Company should fulfil certain obligations with respect to maintenance and preservation of records.

7.1 Maintenance of Records

The Company will put in place appropriate infrastructure and systems to maintain, preserve and report customer information as per applicable law and guidelines provided by RBI or any other relevant regulator from time to time. proper record of the following transactions:

(i) All cash transactions of the value of more than Rupees Ten Lakh;
(ii) Series of all cash transactions individually valued below rupees ten lakh, that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs;
(iii) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine; and
(iv) All suspicious transactions as mentioned in the Rules.

The Company will ensure that following key details of transaction are recorded:

(i) Nature of transaction
(ii) Amount of transaction
(iii) Date on which the transaction was conducted
(iv) Details of parties to the transaction.

7.2 Preservation of Records

The Company shall endeavour to furnish all the information sought by regulatory/ statutory authorities in a time bound manner. Hence, systems will be developed to ensure easy and quick data retrieval.

(i) The Company will maintain for at least 10 years from the date of transaction between the Company and the client, all necessary records of transactions, which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

(ii) Records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business relationship, will be properly preserved for at least 10 years after the business relationship is ended and such records and transaction will be provided to competent authorities upon request.

(iii) Records of the identity of clients and records in respect of transactions will be maintained in both hard as well as soft format.

(iv) The Company will deal with all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose, with utmost due diligence and scrutiny, through branches and AML/KYC team at Head Office. Findings with respect to the aforesaid transactions will be recorded and related documents will be preserved as prescribed under applicable laws and made available to

auditors to scrutinize these transactions.

7.3 Obligation of Secrecy

The Company has an obligation to maintain secrecy of the details of the account holder, not only when the account holder has a relationship with the Company, but also after the account is closed. This right of the customer to expect secrecy is limited in the following situations:

(i) Under provisions of various acts (Income Tax / Companies Act / RBI Act / FEMA Act etc.)
(ii) Based on customer's consent
(iii) Disclosure with Consultants / Business Facilitator
(iv) Disclosure in Company's interest

8. Combating Financing of Terrorism

- The Company shall ensure to update the consolidated list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) circulated by the Reserve Bank.

- The 'ISIL (Da'esh) & Al-Qaida Sanctions List' and '1988 Sanctions List' shall be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967. The Company shall update the lists of individuals/ entities as circulated by Reserve Bank and before opening any new account shall ensure that the name/s of the proposed customer does not appear in either list.

- The Company shall further scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the two lists. Full details of accounts bearing resemblance with any of the individuals/ entities in the list shall immediately be intimated to the Reserve Bank and FIU-IND.

9. Reporting Requirements

9.1. Reporting to Financial Intelligence Unit-India (FIU-IND)

In line with the PMLA rules, the Company shall report information relating to suspicious transactions and to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in rule 3 at the following address:

Director, FIU-IND, Financial Intelligence Unit - India,
6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021.

10. Training and awareness

- The Company shall develop appropriate training literature and display the same at branches and on the website in order to educate the customer about the objectives of KYC/ AML/ CFT programme.
- The Company shall have an ongoing employee training programme so that the members of staff are adequately trained in AML/CFT policy.
- The Company shall also deploy appropriate screening mechanisms while hiring new employees.
- The Company shall ensure implementation and adherence to the Policy via independent evaluation/Concurrent/internal audit system and timely reporting to the Audit Committee ("AC"), administered and complied at the consolidated group

level by Avanti Finance Private Limited, the holding company.

This policy comes into effect immediately on approval by the Board of Directors of the Company and shall remain in force till further review by the Board.

11. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

In terms of provision of Rule 9(1A) of the PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the customer as the case may be.

On receipt of additional or updated information from any customer, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR.

For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless– (i) there is a change in the information of the customer as existing in the records of CKYCR; or (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or (iii) the validity period of downloaded documents has lapsed; or (iv) the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

12. Procedure for change in mobile number of the customer

On receipt of a request from the Customer for change in mobile number existing in the Company's records, the following procedure shall be undertaken:

i. OTP verification of the updation through the existing mobile number or e-signed application from the Customer requesting for a change
ii. OTP verification of the new mobile number
iii. Communication to be sent to the Customer on the old and new mobile numbers

13. Digital KYC Process/Approach

The Company had adopted enhanced KYC process that involves:

(i) its proprietary digital application for undertaking KYC in a secure environment;
(ii) a network of pre-authorized on-ground partners whose whitelisted employees (field officers) have a secured access to the Company's digital application; and
(iii) such partners / field officers (acting in accordance with the Company's instructions) not only assisting for the purpose of KYC but also acting as customer touch-points to inform and educate the customers in relation to the credit facilities and aid in financial literacy.

While the Company's KYC process is in line with the minimum requirements for Digital KYC as set out in Annex I of RBI's Master Direction - Know Your Customer (KYC) Direction, 2016

(DBR.AML.BC.No.81/14.01.001/2015-16) ("**KYC Directions**"), the Company has made a few improvements and modifications to go beyond these minimum requirements so as to make the customer onboarding process more robust and simplified. It is also pertinent to note that while the emphasis is on digital means, the KYC process involves the presence of on-ground authorized officer of the Company who have been authorized to receive copies of customer documents, compare them with the original copy and accept after due verification. This is also verified by the Company from the verification facility of the issuing authority and supplemented with physical verification by the Company's backend team, wherever required.

The KYC process flow adopted by the Company is mentioned under Annexure 4.

14. Policy Review and Updates

The Risk Department shall be responsible to own, maintain and update this policy. If any change in this policy is subsequently found necessary, consequent upon any change in regulatory guidelines, market conditions, etc., such changes and approvals shall be deemed to be part of the policy until the policy and framework are comprehensively reviewed.

15. Regulatory References

This policy is framed according to the following regulatory references:

(i) RBI Master Direction – Know Your Customer (KYC) Direction dated February 25, 2016, as updated from time to time.
(ii) Prevention of Money Laundering Act (PMLA), 2002.
(iii) PML Rules, 2005.

16. Annexures

Annexure 1: Key Definitions

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

   A customer can also be one of the following persons:
   (i) A person or entity that maintains or is desirous of maintaining an account and/or has a business relationship with Company
   (ii) One on whose behalf an account is maintained (i.e. the beneficial owner)
   (iii) Beneficiaries of transactions conducted by professional intermediaries, such as chartered accountants, solicitors, etc. as permitted under the law, and
   (iv) Any person or entity connected with a financial transaction which can pose significant reputational or other risks to Company, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Beneficial Owner:

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

   Explanation- For the purpose of this sub-clause-

   "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.

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

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

   (c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

   (d) Where the **customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

3. Designated Director: "Designated Director" means a person designated by the reporting entity (bank, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes the Managing Director or a whole-time Director duly authorized by the Board of Directors

4. Person: In terms of Prevention of Money Laundering Act, 2002 'a person' includes-

(a) an individual
(b) a Hindu undivided family
(c) a company
(d) a firm
(e) an association of persons or a body of individuals, whether incorporated or not
(f) every artificial juridical person, not falling within any one of the above persons
(g) any agency, office or branch owned or controlled by any of the above persons

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

   (a) opening of an account for the purpose of availing a loan/having a financial arrangement;
   (b) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
   (c) entering into any fiduciary relationship;
   (d) any payment made or received in whole or in part of any contractual or other legal obligation; or
   (e) establishing or creating a legal person or legal arrangement.

6. Money Laundering: A process whereby proceeds of criminal activities such as drugs trafficking, smuggling and terrorism are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds.

7. “Suspicious transaction” means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
   (a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
   (b) appears to be made in circumstances of unusual or unjustified complexity; or
   (c) appears to not have economic rationale or *bona-fide* purpose; or
   (d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Annexure 2 - Documents to be obtained from entities

The details of documents to be obtained from various entities are as under:

Nature of Entity	Documents Required
Individuals	One certified copy of any one of the following Officially Valid Document (OVD), one recent photograph and such other documents as required to ascertain nature of business and financial status of the client. OVD means the passport, the driving licence, the Permanent Account Number (PAN) 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 and Aadhaar number, or any other document as notified by the Central Government in consultation with the regulator. In respect of low risk category customers, where simplified measures are applied, it would be sufficient to obtain a certified copy of any one of the OVDs for the purpose of proof of identity. The additional documents deemed to be OVDs under 'simplified measure' for 'low risk' customers may be obtained for the limited purpose of proof of address. Such OVDs will include the following: (a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) Property or Municipal Tax receipt; (c) Bank account or Post Office savings bank account statement; (d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (e) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, and public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and (f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.
Company	One certified copy of each of the following documents: (a) Certificate of incorporation; (b) Memorandum and Articles of Association; (c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf and (d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf. The Company shall 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.
Partnership Firm	One certified copy of the following documents: (a) Registration certificate;

Nature of Entity	Documents Required
	(b) Partnership deed and (c) An officially valid document in respect of the person holding an attorney to transact on its behalf.
Unincorporated association or a body of individuals	One certified copy of the following documents: (a) Resolution of the managing body of such association or body of individuals; (b) Power of attorney granted to transact on its behalf; (c) An officially valid document in respect of the person holding an attorney to transact on its behalf and (d) Such information as may be required by the Company shall be sought to establish the legal existence of such an association or body of individuals.
Proprietary Concerns	In addition to OVD of individual, any two of the following documents: (a) Registration Certificate including Udyam Registration Certificate (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d) CST / VAT certificate (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. (f) Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. (h) Utility bills such as electricity, water, and landline telephone bills. In case the Company is satisfied that it is not possible for customer to furnish two such documents, it may accept only one of those documents as activity proof. However, the Company shall undertake contact point verification, collect such information as will be required to establish the existence of such firm, confirm, clarify and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Annexure 3: An Indicative List of Suspicious Activities

(i) **Transactions Involving Large Amounts of Cash**

Company transactions that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the Company, e.g. cheques.

(ii) **Transactions that do not make Economic Sense**

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnish a plausible reason for immediate withdrawal.

(iii) **Activities not consistent with the Customer's Business**

Accounts with large volume of credits whereas the nature of business does not justify such credits.

(iv) **Attempts to avoid Reporting/Record-keeping Requirements**

(a) 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.
(b) Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.
(c) An account where there are several cash transactions below a specified threshold level to a 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.

(v) **Unusual Activities**

Funds coming from the countries/centers which are known for money laundering.

(vi) **Customer who provides Insufficient or Suspicious Information**

(a) A customer/Company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.
(b) A customer/Company who is reluctant to reveal details about its activities or to provide financial statements.
(c) A customer who has no record of past or present employment but makes frequent large transactions.

(vii) **Certain NBFC Employees arousing Suspicion**

(a) An employee whose lavish lifestyle cannot be supported by his or her salary
(b) Negligence of employees / wilful blindness is reported repeatedly.

Annexure 4: Digital KYC note

Paragraph	Avanti Workflow	Remarks
A.	Avanti owns a proprietary digital application, access to which is provided to Avanti's authorized partners and field officers. The KYC process is undertaken through this application.	-
B.	Every user needs to be onboarded on the Application. The licensee partner and the field officer's credentials are required to be whitelisted in order to enable them to transact on the Application. Every partner / field officer is provided a unique login ID and password in order to access the Application.	The partner and the field officers are the authorized official, and are duly appointed and authorized pursuant to a Master Services Agreement between the partner and Avanti. The authorized official is then provided access to Avanti application to assist in the KYC process in a secured environment.
C.	The authorized official may visit the customer or the customer may visit the partner's office / branch. Customer is made aware of the OVDs required for the purpose of onboarding and for applying for a loan from Avanti.	-
D.	The platform allows the authorized official to take customer's live photograph which is digitally embedded in a customer application form (CAF) with a unique ID (virtual loan account number). The unique ID is printed on the loan application form. This Application also captures: (i) The GPS coordinates of the location where the photograph is taken; (ii) The authorized official's identity through as he / she is logged into the Application; and (iii) Date Stamp and Time Stamp.	Avanti does not provide watermark of the mentioned details on the customer's photograph for the CAF. However, these details are available in the Application.
E.	The authorized partner ensures that the live photograph does not contain any other person other than the customer. In case of co-borrower, his/her live photograph is captured separately. As discussed, the photograph is captured by use of the device camera in the hands of the authorized official. Avanti prescribes minimum technology standards of such devices which is ensured by Avanti's partner on ground. This is in order to avoid pictures that are grainy, in poor light, against unsuitable or dark backgrounds or otherwise rendered unidentifiable.	While it is encouraged that customer photographs be taken with a white background, Avanti does not reject CAF / customer solely on the ground that such background is absent when all other necessary features under this paragraph (E) are met. CAF with photographs that are not clear or with a photograph of a photograph are rejected during the checking process by the backend team.

F.	Live photographs of the original OVD are captured in a similar manner as described above in case of capturing of live photograph of customer. Authorized partners typically place the OVDs on a plain white surface such as a white paper and then capture its photographs. In case of Aadhaar card, the first eight digits of the Aadhaar number are masked physically by the authorized official.	Please refer to our remarks under D and E above
G.	This is complied with.	Please refer to our remarks under E above
H.	The Application has incorporated a QR code scanner for scanning the demographic details from the Aadhaar card. In case, the scanner does not work (which happens on account of physical condition of the original Aadhaar card or the light conditions or technology misalignment), the authorized official collects the information from the customer such as first and middle name, date of birth, gender, address, mobile number, etc. and inputs it in the Application	The back-end team physically verifies the data with the image of the OVD and mismatches are rejected.
I.	Having captured the details as provided by customer, the authorized official reviews the information for any apparent errors and the same is corrected in consultation with the customer. A validation is built in the Application which does not allow use of the authorized official's mobile number as the mobile number of the customer. On completing the information capture, consent of the customer is taken for pulling the bureau report and for communicating through WhatsApp. This consent is obtained through OTP sent to the mobile number of the customer. It also achieves the purpose of verification of the mobile number of the customer. The customer is once again provided details as to the loan in his/her vernacular language by the authorized official. This process takes place immediately after the details of the customer have been filled in the Application. Once all the information required for CAF including the loan product is captured, a composite CAF and conditional loan agreement is generated. The documents is	Our processes address the concerns with respect to: (a) eliminating risks of use of authorized official's mobile number for OTP (b) establishing the genuine identity of the customer and her physical presence; (c) providing a window for the customer to read, listen to the authorized official's explanation of the loan terms, understand them and accept the terms before signing; (d) meeting the requirements in relation to thumb-impressions (since this is an equivalent of the thumb-impression);and (e) Verification of the phone number of the customer For your reference, Aadhaar e-Sign mode is a recognized electronic signature under the Information Technology Act, 2000 (please refer to Schedule II of the IT Act). Being a statutorily recognized mode of signature that relies on the customer's Aadhaar identification and link to his/her mobile number, it

	signed by the customer through biometric-based Aadhaar e-Sign. The Aadhaar e-Sign returns the name of the customer and the last four digits of the Aadhaar number along with the date and time stamp. The Application compares the name and the last four digits from UIDAI with the name and last four digits captured through scanning or physically filling in the information. Any mismatches are flagged for manual verification and may be rejected if it is proved that the two do not match.	is superior to the non-Aadhaar OTP-based method.
J.	The authorized partner provides a declaration on the Avanti application which he/she must digitally check to proceed with the CAF.	The authorized official's live photograph is not captured and OTP-based verification is not carried out. Nevertheless, each CAF assisted by an authorized official is specifically mapped to such official through the login ID issued to him/her. Thus, verification of the authorized partner is built-in within the process workflow since only whitelisted persons with a unique login ID and password (as provided by Avanti) can access the application. This framework is further strengthened as Avanti has the capability to override / disable any specific login ID if it detects errors or suspicious use of the device
K.	A unique virtual loan account number is generated in the Application and details of the same are shared with the customer by way of SMS / WhatsApp to his/her mobile number. On-ground, the authorized official may also provide these details and recommends to the customer to save it for future reference.	The process is not solely dependent on the authorized official of the partner for communicating the relevant details to the customer. The Application through API integrations ensure real-time sharing of the updates to the customer on their mobile number, at every stage of the loan.
L.	This process is done either through technology integrations or through manual processes by the Avanti backend team.	This is done by the backend operations team.
M.	The Application generates a PDF document which includes the CAF, the image of the OVDs and the conditional loan agreement. This document is signed through Aadhaar based (biometric) e-Sign process.	Customer signature / thumb-impression on printed CAF is not taken since this is a digitally-driven process. However, so far as customer signature is concerned, please refer to the process

	The document with digital signature of Avanti and e-Sign of the borrower, co-borrower and guarantors (if applicable) is also shared with the borrow through SMS / WhatsApp	workflow and our comments at paragraph (I) above. CAF is not digitally signed by the authorized official since it is already mapped to the authorized official as part of the process flow and secured access is ensured.