



**AAVAS FINANCIERS LIMITED
POLICY ON “KNOW YOUR CUSTOMER” AND
“ANTI-MONEY LAUNDERING MEASURES”**



**AAVAS FINANCIERS LIMITED
POLICY ON KNOW YOUR CUSTOMER & ANTI MONEY LAUNDERING MEASURES**

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

Version Control

Document Version	Description of change	Date	Prepared by	Approved/ Review
1.0	First Approval	March 10, 2012	Compliance	Board
1.0	Reviewed	May 30, 2013	Compliance	Board
1.0	Reviewed	May 23, 2014	Compliance	Board
1.0	Reviewed	May 27, 2015	Compliance	Board
1.1	Reviewed	May 26, 2016	Compliance	Board
1.1	Reviewed	May 26, 2017	Compliance	Board
1.1	Reviewed	April 27, 2018	Compliance	Board
1.2	Amended	May 03, 2019	Compliance	Board
1.2	Reviewed	May 14, 2020	Compliance	Board
1.3	Amended	August 12 ,2020	Compliance	Board
1.3	Reviewed	July 28, 2022	Compliance	Board
1.4	Amended	February 02, 2023	Compliance	Board
1.5	Amended	August 03, 2023	Compliance	Board
1.5	Reviewed	February 01, 2024	Compliance	Board
1.5	Reviewed	January 30, 2025	Compliance	Board
1.5	Reviewed	February 05, 2026	Compliance	Board
1.6	Amended	July 21, 2026	Compliance	Board

1. Introduction & Regulatory Framework

(i) Aavas Financiers Limited (“**the Company/Aavas**”) is a Housing Finance Company, regulated by Reserve Bank of India (RBI), under the supervision of National Housing Bank (NHB). Accordingly, this Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy (“Policy”) is formulated in compliance with the following laws, rules, and regulatory directions as amended from time to time:

- Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 as applicable to Housing Finance Companies (HFCs) (“RBI Master Direction),
- Prevention of Money-Laundering Act, 2002 (“PMLA”),
- Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (“PML Rules”), and
- Applicable circulars, notifications, guidelines, and clarifications issued by RBI, NHB and other statutory authorities.

(ii) The objective of this Policy is to:

- To ensure all necessary Customer Identification Procedures (“CIP”) / Customer Due Diligence (“CDD”)/ Enhanced Due Diligence (“EDD”) measures are followed.
- To reflect Company’s approach to customer due diligence, risk management, record keeping, and reporting obligations.
- To prevent the Company from being used, intentionally or unintentionally, for money laundering, terrorist financing, or proliferation financing.
- To enable the Company to understand its customers and their financial dealings.
- To establish appropriate risk-based controls and due diligence measures.
- To ensure full compliance with applicable regulatory and statutory requirements.

(iii) This Policy has been approved by the **Board of Directors of Aavas Financiers Limited**.

(iv) All extant & future circulars/directions/guidelines/guidance notes issued by NHB/ RBI/ any other regulatory authority, from time to time would be the directing force for the KYC AML Policy of the Company and will supercede the contents of this Policy.

2. Definitions

The terms used and not defined in this Policy shall have the same meaning as assigned to them in the RBI Master Direction, as amended from time to time.

(i) ‘**Act**’ and ‘**Rules**’ mean the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

(ii) ‘**Beneficial Owner (BO)**’:

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

Explanation: For the purpose of this sub-clause-

- ‘Controlling ownership interest’ means ownership of / entitlement to more than 10 percent of the shares or capital or profits of the company.

AAVAS FINANCIERS LIMITED

POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

- ‘Control’ shall include the right to appoint the 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 BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has / have ownership of / entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.
Explanation: For the purpose of this sub-clause, ‘control’ shall include the right to control the management or policy decision.
 - c) Where the **customer is an unincorporated association or body of individuals**, the BO 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 percent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term ‘body of individuals’ includes societies. Where no natural person is identified under (a), (b) or (c) above, the BO is the relevant natural person who holds the position of senior managing official.
 - d) Where the **customer is a trust**, the identification of BO(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 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.
- (iii) **‘Certified Copy’** obtaining the certified copy shall mean comparing the copy of the proof of possession of Aadhaar number (where offline verification cannot be carried out) or the officially valid document produced by the customer with the original, and an authorised officer of the Company shall record the comparison on the copy as per the provisions contained in the Act. Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:
- a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
 - b) branches of overseas banks with whom Indian banks have relationships,
 - c) Notary Public abroad,
 - d) Court Magistrate,
 - e) Judge,
 - f) Indian Embassy / Consulate General in the country where the non-resident customer resides.
- (iv) **‘Central KYC Records Registry (CKYCR)’** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- (v) **‘Customer’** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- (vi) **‘Customer Due Diligence (CDD)’** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.
Explanation: The CDD, shall include:
- a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
 - b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
 - c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.



AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

(vii) **‘Customer identification’** means undertaking the process of CDD.

(viii) **‘Designated Director’** means a person designated by Board of Directors of the Company to ensure compliance with obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director.

(ix) **‘Digital KYC’** means that an authorised officer of the Company captures a live photo of the customer and officially valid document or the proof of possession of Aadhaar (where offline verification cannot be carried out), along with the latitude and longitude of the location where such live photo is being taken, as per the provisions contained in the Act.

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

(xi) **‘Know Your Client (KYC) Identifier’** means the unique number or code that the Central KYC Records Registry assigns to a customer.

(xii) **‘Non-face-to-face customers’** means customers who open accounts without visiting the branch / offices of the NBFC or meeting the officials of the Company.

(xiii) **‘Officially Valid Document (OVD)’** means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card that the Election Commission of India issues, the job card that NREGA issues and an officer of the State Government duly signs, and the letter that the National Population Register issues containing details of name and address.

Provided that,

- a) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form that the Unique Identification Authority of India (UIDAI) issues.
- b) When the customer furnishes an OVD that does not have an updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: -
 - utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - property or Municipal tax receipt;
 - pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - letter of allotment of accommodation from employer that is issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
- c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at (b) above.

Explanation: For the purpose of this clause, the Company shall deem a document to be an OVD even if there is a change in the name subsequent to its issuance provided that it is supported by a marriage certificate that the State Government issues or a Gazette notification, indicating such a change of name.

(xiv) **‘Offline verification’** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) (“Aadhaar Act”).

(xv) **‘On-going Due Diligence’** means regular monitoring of transactions in accounts to ensure that transactions are consistent with the Company’s knowledge about the customers, customers’ business and risk profile, the source of funds / wealth.

(xvi) **‘Periodic Updation’** means the steps taken to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the RBI.

(xvii) **‘Person’** has the same meaning assigned in the Act and includes:

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

(xviii) **‘Principal Officer’** means an officer appointed by Board of Directors of the Company, at the management level, responsible for furnishing information as per rule 8 of the Rules.

(xix) **‘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 have no 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.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds that the NBFC suspects are linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism. (xix) ‘Transaction’ means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

(xx) **‘Video based Customer Identification Process (V-CIP)’**: An alternative method by which an authorised official of the Company conducts customer identification with facial recognition and customer due diligence. This process involves a seamless, secure, live, informed- consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information which the customer furnished, through independent verification and by maintaining an audit trail of the process.

(xxii) **‘Walk-in Customer’** means a person who does not have an account-based relationship with the Company, but undertakes transactions with it.

3. Elements of Policy

The KYC policy includes following four key elements:

- (i) Customer Acceptance Policy
- (ii) Risk Management
- (iii) Customer Identification Procedures (CIP); and

- (iv) Monitoring of Transactions

4. Customer Acceptance Policy

Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, the Company shall ensure that:

- (i) No account is opened in anonymous or fictitious/benami name;
- (ii) No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- (iii) No transaction or account-based relationship is undertaken without following the CDD procedure.
- (iv) Customer/ Authorised signatory must be a major (i.e., 18 years or above) and must not be incapacitated for entering into a contract as per Indian Contract Act.
- (v) Name / identity of the customer/ Authorised signatory/ Beneficial owner should not appear / match with any person or entity, whose name appears in the sanctions lists / designated lists/ other lists as circulated by United Nations Security Council (UNSC) / RBI / FIU-IND / any other regulatory authority, as amended from time to time.
- (vi) The mandatory information to be sought for KYC purpose while opening a loan account and during the periodic updation, are as specified in this policy.
- (vii) Optional additional information, is obtained with the explicit consent of the customer after the loan account is opened.
- (viii) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with customers (individual as well as non-individuals) as also the existing customers.
- (ix) The Company shall apply the CDD procedure at the Unique Customer Identification Customer (UCIC) level. Thus, if an existing KYC-compliant customer of the Company desires to open another account or avail of 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.
- (x) CDD Procedure is followed for all the joint loan account holders, while applying in joint.
- (xi) Circumstances in which, a customer is permitted to act on behalf of another person/ entity, are clearly spelt out in the policy.
- (xii) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- (xiii) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.
- (xiv) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority
- (xv) Customer / Authorised signatory/Beneficial Owner classified as fraud by the Company or any other financial entity regulated by RBI or also entities and persons associated with such entities shall be treated as per the board approved Fraud Risk Management Policy.

It is important to note that the adoption of Customer Acceptance Policy and its implementation should not result in denial of services to general public, especially to those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs).

Where, the Company forms a suspicion of money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report ("STR") with FIU-IND

5. Risk Management

For Risk Management, the Company shall have a risk-based approach which includes the following:

- (i) Customers shall be categorized as low, medium and high-risk category, based on the assessment and Risk perception of the Company..
- (ii) These principles shall be based on parameters such as customer's identity, social/ financial status, nature of business activity and information about the 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.
- (iii) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
- (iv) Indicative list of customers for Risk Categorization: -

✓ **Low Risk**

- 1. All Salaried employment getting salary in bank account.
- 2. All Self-employed with documented income
- 3. All Salaried/Self-employed with informal income/non documented income with Loan exposure of Rs 50 lacs
- 4. Cash Transaction below 2 lacs cumulatively

✓ **Medium Risk**

- 1. All Salaried/Self-employed with informal income/non documented income with Loan exposure of Rs 50 lacs to 100 Lacs
- 2. Cash transactions more than Rs.2 Lakhs but up to Rs.5 lakhs cumulatively

✓ **High Risk**

- 1. Politically Exposed Persons (PEP)
- 2. Loans to Non-Resident Indian (NRI)
- 3. Non-Face-to-Face onboarding customer
- 4. Appeared anytime in sanction / watch lists
- 5. Ever reported to FIU-IND
- 6. Loans to Trusts, Societies, NGOs and organizations receiving donations.
- 7. All Salaried/Self-employed with informal income/non documented income with Loan exposure more than 100 lacs
- 8. Cash transactions exceeding Rs.5 Lakhs cumulatively

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in this policy.

The Company may use the Financial Action Task Force (FATF) Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies etc. in its risk assessment.

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

5A. Money Laundering and Terrorist Financing Risk Assessment by the Company:

- (i) The Company shall carry out ‘Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment’ exercise periodically (at least annually) to identify, assess and take effective measures to mitigate its money laundering terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
- (ii) The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
- (iii) The risk assessment shall be properly documented, and it shall be proportionate to the nature, size, geographical presence, complexity of activities / structure, etc. of the Company.
- (iv) The outcome of the exercise shall be put up to the Risk Management committee of the Board and should be available to competent authorities and self-regulating bodies.
- (v) The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk, in line with this policy. The Company shall implement a CDD programme, having regard to the ML/TF risks identified (by the Company itself) and the size of business, for mitigation and management of the identified risk. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

6. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

The Company shall undertake identification of customers in the following cases:

- (i) Commencement of an account-based relationship with the customer.
- (ii) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on CDD done by a third party, subject to the following conditions:

- (i) The Company shall immediately obtain records or the information of the customer due diligence carried out by the third party either from the third party or from the CKYCR records.
- (ii) The Company shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- (iii) The third party is regulated, supervised or monitored, and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- (iv) The third party is not based in a country or jurisdiction assessed as high risk.
- (v) The Company is ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

While undertaking customer identification through third parties, the Company shall ensure that the decision-making functions of determining compliance with KYC norms are not outsourced.

6A. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

Part- I CDD Procedure in case of individuals

The Company shall obtain the following from an individual while carrying out CIP or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

- (i) the Aadhaar number, where
 - a) they are desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act; or
 - b) they decide to submit their Aadhaar number voluntarily to the Company; or

Provided that, the Company shall carry out authentication of the customer's Aadhaar number using UIDAI's e-KYC authentication facility. Further, in such a case, if customer wants to provide a current address, different the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect.

- (ii) the proof of possession of Aadhaar number where offline verification can be carried out; or
Provided that, the Company shall carry out such offline verification.
- (iii) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or

Provided that, in case customer submits an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Digital KYC Process and its rules and regulations reproduced under **Annexure-A**.

Provided further that in case customer submits any OVD or proof of possession of Aadhaar number, where offline verification cannot be carried out, the Company shall carry out verification through digital KYC process and its rules and regulations reproduced under **Annexure-A**.

- (iv) the KYC Identifier with an explicit consent to download records from CKYCR;
Provided that the Company shall retrieve the KYC records online from the CKYCR in accordance with the rules prescribed for sharing KYC information with CKYCR.
and
- (v) the PAN or the equivalent e-document thereof or Form No. 97 as defined in Income-tax Rules, 1962; and
- (vi) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company as per its Credit Policy.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Company may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the internal audit. The Company shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection and shall be available for supervisory review.

V-CIP process, as prescribed under the RBI Master Direction from time to time, may also be carried out as part of customer identification process, if deemed appropriate.



AAVAS FINANCIERS LIMITED

POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

Explanation 1: The Company shall, where its customer submits a proof of possession of 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.

Explanation 2: The Company can perform biometric based e-KYC authentication, including Aadhaar Face Authentication.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar Act and the regulations made thereunder.

Explanation 4: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act, the customer shall provide the Aadhaar number. In other cases, customers may provide the Aadhaar number voluntarily.

KYC verification once done by one branch of the Company shall be valid for transfer of the account to any other branch of the Company, provided the Company has already completed the full KYC verification for the concerned account and the same is not due for periodic updation.

Part- II CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, the Company shall carry out the CDD of the individual (proprietor).

In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

- a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
- b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
- c) Sales and income tax returns.
- d) CST/VAT/GST certificate.
- e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
- f) IEC (Importer Exporter Code) issued to the 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.
- 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 cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/activity.

Provided that the Company undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part- III CDD Measures for Legal Entities

- (i) For opening an account of a company, the Company shall obtain certified copy of each of the following documents:
 - a) Certificate of incorporation;
 - b) Memorandum and Articles of Association;
 - c) PAN of the company;
 - d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

- e) Documents, as required for CDD Procedure in case of individuals, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
 - f) The names of the relevant persons holding senior management position;
 - g) The registered office and the principal place of its business, if it is different.
- (ii) For opening an account of a partnership firm, the Company shall obtain certified copy of each of the following documents:
- a) Registration certificate;
 - b) Partnership deed;
 - c) PAN of the partnership firm;
 - d) Documents, as required for CDD Procedure in case of individuals, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
 - e) the names of all the partners;
 - f) address of the registered office, and the principal place of its business, if it is different.
- (iii) For opening an account of a trust, the Company shall obtain certified copy of each of the following documents:
- a) Registration certificate;
 - b) Trust deed;
 - c) PAN or Form No.97 of the trust;
 - d) Documents, as required for CDD Procedure in case of individuals, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
 - e) The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
 - f) The address of the registered office of the trust; and
 - g) List of trustees and documents, as required for CDD Procedure in case of individuals, for those discharging role as trustee and authorized to transact on behalf of the trust.
 - h) In case a customer is non-profit organisations, it shall be registered on the DARPAN Portal of NITI Aayog. If it is not registered, the Company shall register the details on the DARPAN Portal.
- (iv) For opening an account of an unincorporated association or a body of individuals, the Company shall obtain certified copy of each of the following documents:
- a) Resolution of the managing body of such association or body of individuals;
 - b) PAN or Form No.97 of the unincorporated association or a body of individuals;
 - c) Power of attorney granted to transact on its behalf;
 - d) Documents, as required for CDD Procedure in case of individuals, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
 - e) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.
- Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals', includes societies
- (v) For opening accounts of juridical persons (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats etc., or who purports to act on behalf of such juridical person or individual or trust, the Company shall obtain certified copy of each of the following documents:
- a) Document showing name of the person authorised to act on behalf of the entity;
 - b) Documents, as required for CDD Procedure in case of individuals, of the person holding an attorney to transact on its behalf and

- c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Part-IV CDD Measures for Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his/her identity shall be undertaken keeping in view the following:

- (i) Where the customer or the owner of the controlling interest is:
 - a) an entity listed on a stock exchange in India, or
 - b) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
 - c) 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.
- (ii) In cases of trust/nominee or fiduciary accounts, whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

7. Monitoring of Transactions

7A. On-going Due Diligence Measures

The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds/wealth.

Without prejudice to the generality of factors that call for close monitoring, following types of transactions shall necessarily be monitored:

- (i) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- (ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.

For on-going due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI and ML) technologies to support effective monitoring. The extent of monitoring shall be aligned with the risk category of the customer.

A system of periodic review of risk categorisation of accounts at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. High risk accounts have to be subjected to more intensified monitoring.

7B. Reporting to Financial Intelligence Unit – India (FIU-IND)

The Company shall comply with the reporting requirements prescribed under the PML Act and the PML Rules, and shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), all information relating to transactions specified under Rule 3, in accordance with Rule 7 thereof and the guidelines issued by FIU-IND from time to time.

The Company shall adhere to the prescribed reporting formats, reporting format guides, and utilise the Report Generation Utility and Report Validation Utility or other electronic utilities made available by FIU-IND for timely

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

filing of Cash Transaction Reports (CTR), Suspicious Transaction Reports (STR) and Counterfeit Currency Report (CCR).

The Principal Officer shall ensure appropriate arrangements for collection and electronic submission of transaction data, including from non-computerised branches, if any. Any delay in reporting or rectification of misreported transactions beyond the prescribed timelines shall be treated as a separate violation for each day of delay. Filing of STRs shall not result in restriction of customer account operations. The Company, its directors, officers and employees shall maintain strict confidentiality regarding the maintenance and furnishing of records to FIU-IND, without prejudice to internal sharing of analysis of unusual or suspicious transactions as permitted under applicable directions.

The Company shall also report the details of accounts resembling any of the individuals/entities in the sanction lists as per Para 7C and 7D below to FIU-IND.

7C. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967

The Company shall ensure that in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals / entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC), namely the 'ISIL (Da'esh) & Al-Qaida Sanctions List' and the 'Taliban Sanctions List (1988 Sanctions List)'.

The Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The Company shall verify the aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, on a daily basis, and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

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

7D. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)

The Company shall ensure compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India. The Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

Customers shall be screened at onboarding and on an ongoing basis against the designated lists issued by FIU-India, applicable other UNSCRs, and relevant schedules under the UAPA, 1967, and no transactions shall be carried out where a match is identified.

In case of a match or where there is reason to believe that funds or assets fall within the scope of Section 12A of the WMD Act, the Company shall immediately prevent transactions, report full particulars to the Central Nodal Officer (Director, FIU-IND) with copies to the State Nodal Officer and RBI, and promptly comply with all directions relating to freezing or unfreezing of assets in accordance with the prescribed procedure.

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

The Company shall verify every day, the ‘UNSCR 1718 Sanctions List of Designated Individuals and Entities’, to take into account any modifications to the list and also ensure compliance with the ‘Implementation of Security Council Resolution on Democratic People’s Republic of Korea Order, 2017’, as amended from time to time.

8. Updation/ Periodic Updation of KYC

For the purpose of effective monitoring of KYC, the Company shall adopt a risk-based approach for periodic updation of KYC, ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk.

The Company shall carry out periodic updation of KYC as per below grid from the date of opening of the account / last KYC updation, as per the following procedure:

Risk Category	Periodic Updation of KYC
High	2 years
Medium	8 years
Low	10 years

(i) Individuals:

No change in KYC information: In such case, the Company shall obtain a self-declaration in this regard from the customer through the Aavas Loan App or by logging into the loan account on the Aavas website, using the mobile number registered with the Company.

Change in address or KYC information: In such case, the Company shall obtain a copy of OVD, deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation / periodic updation. Customers can submit a copy of OVD by personally visiting any branch of the Company.

The Company may also use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with it in the customer’s profile, in order to prevent any fraud.

(ii) Customers other than individuals:

No change in KYC information: In such case, the Company shall obtain a self-declaration in this regard from the customer through the Aavas Loan App or by logging into the loan account on the Aavas website, using the mobile number or email id registered with the Company. Further, the Company shall ensure during this process that Beneficial Ownership information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

Change in KYC information: In such case, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new customer.

(iii) Additional measures: In addition to the above, the Company shall ensure that:

- a) The KYC documents of the customer as per the current CDD standards are available with them. 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.

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

- b) The Company shall verify the Customer’s PAN details, if available, from the database of the issuing authority.
- c) Acknowledgment is 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.
- d) The facility of updation / periodic updation of KYC is available at all branches.
- e) The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship/ account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents within 30 days for the purpose of updating the records at Company’s end.
- f) Due Notices for Periodic Updation of KYC (With effect from January 1, 2026)
 - At least three advance intimations (1 by letter) prior to the due date and at least 3 reminders (1 by letter) after the due date shall be sent to the customers.
 - Such intimations/ reminders shall be duly recorded for audit trail.
 - The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time.
- g) Periodic Updation of KYC shall be carried out at the UCIC level.

In case of existing customers, the Company shall obtain the PAN or equivalent e-document thereof or Form No.97, by such date as may be notified by the Central Government, failing which the Company shall temporarily cease operations in the account until the customer submits the PAN or equivalent e-documents thereof or Form No. 97.

Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, appropriate relaxation(s) shall be given, as per internal policy, for continued operation of accounts for customers who are unable to provide PAN or equivalent e-document thereof or Form No. 97 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 gives in writing to the Company that he does not want to submit his PAN or equivalent e-document thereof or Form No.97, 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.

For the purpose of this Section, “temporary ceasing of operations” in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account till such time the customer complies with the provisions of this Section.

9. Compliance of KYC policy:

- (i) 'Senior Management' for the purpose of KYC compliance shall mean:
 - a) Chief Credit Officer, for ensuring implementation of KYC policies and procedures and ensuring compliance with the regulatory guidelines on KYC/ AML issued from time to time.
 - b) Head of Operations, for maintaining all KYC records of the borrowers.
- (ii) Allocation of responsibility for effective implementation of policies and procedures.
- (iii) The Company shall ensure independent evaluation of the compliance functions of its policies and procedures, including legal and regulatory requirements.
- (iv) The internal auditor needs to quarterly update to the Audit Committee on the compliance with KYC/Anti-Money Laundering (AML) policies and procedures.
- (v) Audit Committee shall be reported in the form of a note on a quarterly basis about the status of KYC Compliance in accordance with this policy.
- (vi) The Company shall ensure that the decision-making functions of determining compliance with KYC norms are not outsourced.

10. Enhanced Due Diligence Procedure (EDD)

10A. EDD in case of Non-face-to-face customer onboarding:

Non-face-to-face onboarding would include customer onboarding without meeting the customer physically or through V-CIP. Non-face-to-face would include use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs, where there is no physical interaction with the customer.

Following EDD measures shall be undertaken by the Company for non-face-to-face customer onboarding.

- (i) V-CIP shall be provided as the first option to the customer for remote onboarding.
- (ii) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
- (iii) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation such as address verification letter, contact point verification, deliverables, etc. before disbursement of the loan.
- (iv) PAN shall be mandatory in such cases and it shall be verified from the verification facility of the issuing authority.
- (v) The Company shall ensure that first transaction in such accounts is a credit from existing KYC-complied bank account of the customer.
- (vi) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to face manner or through V-CIP.

10B. Accounts of Politically Exposed Persons (PEPs):

- (i) The company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that apart from performing normal customer due diligence:
 - a) The Company has in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
 - b) Reasonable measures are taken by the Company for establishing the source of funds / wealth;
 - c) the approval to open an account for a PEP is taken from the senior management.

- d) all such accounts are subjected to enhanced monitoring on an on-going basis;
- e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
- (ii) These instructions shall also be applicable to family members or close associates of PEP.

Explanation: For the purpose of this paragraph, “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.”

10C. Customer's accounts opened by Professional Intermediaries

The Company shall ensure while opening customer's accounts through professional intermediaries, that:

- (i) Customer shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (ii) The Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- (iii) The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the HFC.
- (iv) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of HFC, the Company shall look for the beneficial owners.
- (v) The Company shall, at their discretion, rely on the CDD done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- (vi) The ultimate responsibility for knowing the customer lies with the Company.

10D. Jurisdictions that do not or insufficiently apply the FATF Recommendations

The Company shall consider the FATF Statements circulated by the RBI from time to time, and publicly available information, to identify jurisdictions that do not or insufficiently apply the FATF Recommendations. The Company shall apply enhanced due diligence measures, commensurate with the assessed risks, to business relationships and transactions involving natural or legal persons (including financial institutions) from such jurisdictions, and shall give special attention to such relationships and transactions. The Company shall examine the background and purpose of these transactions, maintain written records of its findings along with supporting documentation, and make the same available to the RBI or other relevant authorities upon request, without restricting legitimate trade or business activities.

11. Record Management

The Company shall take the following steps regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules.

- (i) Records of all transactions between the Company and the customers, shall be maintained for a period of at least 5 years from the date of transaction, including but not limited to, the nature of the transactions, the amount of the transaction and the currency in which it was denominated, the date on which the transaction was conducted and the parties to the transaction.
- (ii) The records pertaining to the identification of the customers and their addresses, obtained while opening the account and during the course of business relationship and also the registration records on DARPAN portal (if any) etc., shall be preserved as per the Loan Document Records Retention Policy of the Company.

The company shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Such records can be maintained in hard or soft format, and swiftly be made available, to the competent authorities upon request.

12. Other General Guidelines

(i) Appointment of Principal Officer

The Board of Directors of the Company has designated ‘Chief Compliance Officer’ as the Principal Officer. Principal Officer shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The name, designation, address, and contact details of the Principal Officer shall be communicated to the FIU-IND and RBI.

(ii) Appointment of Designated Director

The Board of Directors of the Company has appointed ‘Managing Director & Chief Executive Officer’ (MD & CEO) as the Designated Director. The Designated Director shall be responsible for ensuring overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. The name, designation, address, and contact details of the Principal Officer shall be communicated to the FIU-IND and RBI.

(iii) Secrecy Obligations and Sharing of Information:

- a) The Company shall maintain secrecy regarding the customer information that arises out of the contractual relationship between the Company and the customer.
- b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- c) While considering the requests for data/information from Government and other agencies, the Company shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in transactions.
- d) The exceptions to the said rule shall be as under:
 - where disclosure is under compulsion of law
 - where there is a duty to the public to disclose,
 - where the interest of the Company requires disclosure and
 - where the disclosure is made with the express or implied consent of the customer.

(iv) Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

The Company shall comply with the Foreign Contribution (Regulation) Act, 2010, its Rules, and any related instructions or communications issued by the RBI or Ministry of Home Affairs from time to time.

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

- a) The Company shall capture the customer’s KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer, in the manner mentioned in the Rules, as per the KYC templates prepared for ‘Individuals’ and ‘Legal Entities’ (LEs).

Operational Guidelines for uploading the KYC data are released by Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

- b) Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual / LE as the case may be.

AAVAS FINANCIERS LIMITED

POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

- c) Whenever the Company obtains additional or updated information from existing customer, it shall furnish the updated information to CKYCR within seven days.
- d) For the purpose of establishing an account-based relationship, updation/ periodic updation, 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 from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
 - there is a change in the information of the customer as existing in the records of CKYCR; or
 - the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - the validity period of downloaded documents from CKYCR has lapsed; or
 - 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

(vi) Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

The NBFC shall comply with the provisions of Income Tax Rules 238, 239, and 240 under FATCA and CRS, including determining its status as a Reporting Financial Institution. It shall register on the Income Tax e-filing portal, carry out due diligence to identify reportable accounts using FEDAI reference rates, maintain records through an IT framework, and submit online reports (Form 166 or NIL) signed by the Designated Director. A High-Level Monitoring Committee shall oversee compliance, and the NBFC shall adhere to all updated instructions, guidance notes, and press releases issued by the CBDT.

(vii) Operation of accounts and Money Mules

The Company shall follow strict procedures for account opening and transaction monitoring to prevent the use of accounts as “Money Mules” in fraud schemes. Diligence and ongoing monitoring shall be conducted to identify such accounts, and appropriate action, including reporting of suspicious transactions to FIU-IND, shall be taken.

(viii) Introduction of New Technologies

The Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Further, the Company shall ensure: (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

(ix) Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 159 applicable to banks, as amended from time to time. Form 97 (as per Income Tax Rules 2026) shall be obtained from persons who do not have PAN or equivalent e-document thereof.

(x) Hiring of Employees and Employee training

- a) The Company shall put in place adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process should be put in place to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have high integrity and ethical



AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

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 and also develop an environment which fosters open communication and high integrity amongst the staff.

- b) On-going employee training programme should be put in place so that the members of staff are adequately trained in KYC/AML Measures policy. The focus of the training should be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff should 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 Measures policies, regulation and related issues should be ensured.

AAVAS FINANCIERS LIMITED POLICY ON “KNOW YOUR CUSTOMER” AND “ANTI-MONEY LAUNDERING MEASURES”

Annexure - A Digital KYC Process

- (i) The Company shall develop an application for digital KYC verification process as far as possible, which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.
- (ii) The Company shall control the access to the Application and shall ensure that unauthorised persons do not use it. Authorised officials shall access the Application only through a login-id and password or a Live OTP or Time OTP controlled mechanism that the Company provides.
- (iii) The customer, for the purpose of KYC, shall visit the location of the authorised official of the Company or vice-versa. The original OVD shall be in possession of the customer.
- (iv) The Company shall ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by the Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- (v) The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- (vi) Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
- (vii) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- (viii) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
- (ix) Once the above- mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
- (x) The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
- (xi) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction id/reference-id number to customer for future reference.
- (xii) The authorized officer of the Company shall check and verify that a) information available in the picture of document is matching with the information entered by authorized officer in CAF. b) live photograph of the customer matches with the photo available in the document.; and c) all of the necessary details in CAF including mandatory field are filled properly. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.