

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

PREAMBLE

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Housing Finance Companies (HFCs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions. **Aavas Financiers Limited (“AAVAS”)** shall take steps to implement provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

1. DEFINITIONS:

In these Guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:-

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

- **"Aadhaar number"** means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act';
- **"Act"** and **"Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto;
- **"Authentication"** means the process as defined under sub-section (c) of section 2 of the Aadhaar Act;
- **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 person, has/have a controlling ownership interest or who exercise control through other means.

For the purpose of this sub-clause:-

"Controlling ownership interest" means ownership of/entitlement to more than 25 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 BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership off entitlement to more than 15per cent of capital or profits of the partnership.

(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 off entitlement to more than 15 percent of the property or capital or profits of the Unincorporated Association or Body of Individuals.

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 shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person

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

exercising ultimate effective control over the trust through a chain of control or ownership.

- **“Certified Copy”** - Obtaining a certified copy by the RE shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE 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:
 - authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
 - branches of overseas banks with whom Indian banks have relationships,
 - Notary Public abroad,
 - Court Magistrate,
 - Judge,
 - Indian Embassy/Consulate General in the country where the non-resident customer resides
- **“Designated Director”** means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:
 - a. person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:
 - a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
 - b. the Managing Partner, if the RE is a partnership firm,
 - c. the Proprietor, if the RE is a proprietorship concern,
 - d. the Managing Trustee, if the RE is a trust,
 - e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
 - f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

- **Digital KYC”** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the AAVAS as per the provisions contained in the Act.
- **“Digital Signature”** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
 - **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation

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

and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

- **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
- **"KYC identifiers"** means unique number or code assigned to a customer by the Central KYC Records Registry Non-profit organisations" (NPO) means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.
- **"Officially Valid Document" (OVD)** means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents there of shall be deemed to be OVDs for the limited purpose of proof of address:-

- i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii. property or Municipal tax receipt;
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer 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
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

- "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).
- **"Person"** has the same meaning as defined in the Act and includes:
 - a) an individual,
 - b) a Hindu undivided family,
 - c) a company,

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

- 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 anyone of the above persons (a to e), and
- g) any agency, office or branch owned or controlled by any of the above persons (a to f).

- **"Principal Officer"** means "Principal Officer" nominated by the RE, responsible for furnishing information as per rule 8 of the Rules
- **"Suspicious Transaction"** means 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;
 - orb. appears to be made in circumstances of unusual or unjustified complexity;
 - orc. appears to not have economic rationale or bona-fide purpose;
 - ord. 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 suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.
- **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
 - a. opening of an account;
 - b. deposit, 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. the use of a safety deposit box or any other form of safe deposit;
 - d. entering into any fiduciary relationship;
 - e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
 - f. establishing or creating a legal person or legal arrangement.
- **"Video based Customer Identification Process (V-CIP)"**: a method of customer identification by an official of the AAVAS by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:
- **"Common Reporting Standards" (CRS)** means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
- **"Customer"** means a person who is engaged in a financial transaction or activity with a RE and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- **"Walk-in Customer"** means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
- **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner. v. "Customer identification" means undertaking the process of CDD.

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

- **“FATCA”** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
- **“IGA”** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
- **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- **“Non-face-to-face customers”** means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.
- **“On-going Due Diligence”** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.
- **“Periodic Updation”** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- **“Politically Exposed Persons” (PEPs)** are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- **“Regulated Entities” (REs)** means a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as ‘banks’b. All India Financial Institutions (AIFIs)c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
- **“Shell bank”** means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
- **“Wire transfer”** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.
- **“Domestic and cross-border wire transfer”**: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator bank’ or ‘beneficiary bank’ is located in different countries such a transaction is cross-border wire transfer.

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

(c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the 14Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

GENERAL

2. Know Your Customer (KYC) Policy:

2.1. The policy of AAVAS includes following key elements:

- (a) Customer Acceptance Policy;
- (b) Risk Management;
- (c) Customer Identification Procedures (CIP); and
- (d) Monitoring of Transactions

3. Money Laundering and Terrorist Financing Risk Assessment by AAVAS:

(a) AAVAS shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, AAVAS shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with AAVAS from time to time.

(b) The risk assessment by the AAVAS shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the AAVAS. Further, the periodicity of risk assessment exercise shall be determined by the Board of the AAVAS, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

AAVAS shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, AAVAS shall monitor the implementation of the controls and enhance them if necessary.

4. Designated Director:

- (a) A "Designated Director" means a person designated by the AAVAS to ensure overall compliance with the obligations imposed under **Section Risk Management** of the Policy and nominated by the Board of the AAVAS.
- (b) The name, designation and address of the Designated Director, including changes from time to time, shall be communicated to the Director, FIU-IND and also to the National Housing Bank.
- (c) In no case, the 'Principal Officer' shall be nominated as the 'Designated Director'.

5. Principal Officer:

- (a) AAVAS shall appoint a "Principal Officer" (Preferably of the level of General Manager or immediately below the level of CMD/ED of the AAVAS).

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

- (b) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- (c) The name, designation and address of the Principal Officer, including changes from time to time, shall be communicated to the Director, Financial Intelligence Unit - India (FIU-IND) and also to the National Housing Bank.

6. Compliance of KYC policy:

AAVAS shall ensure compliance with KYC Policy through:

- (a) Specifying as to 'Senior Management' for the purpose of KYC compliance;- **Ripudaman Bandral, Chief Credit Officer**
- (b) Allocation of responsibility for effective implementation of policies and procedures;
- (c) Independent evaluation of the compliance functions of AAVAS policies and procedures, including legal and regulatory requirements.
- (d) Concurrent/internal audit system to verify the compliance with KYC/Anti-Money Laundering (AML) policies and procedures.
- (e) Submission of quarterly audit notes and compliance to the Audit Committee.

Aavas ensured that decision-making functions of determining compliance with KYC norms are not outsourced.

7. CUSTOMER ACCEPTANCE POLICY

The AAVAS shall have to ensured and placed elaborate standard procedures on the following aspects of customer relationships in Company, without prejudice:

- a) No account is opened in anonymous or fictitious/benami name;
- b) No account is opened where the AAVAS 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.
- c) No transaction or account based relationship is undertaken without following the CDD procedure.
- d) The mandatory information to be sought for KYC purpose while opening an loan account and during the periodic updation, is specified.
- e) Optional additional information, is obtained with the explicit consent of the customer after the loan account is opened.
- f) AAVAS shall apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of a AAVAS desires to open another account with the AAVAS, there shall be no need for a fresh CDD exercise.
- g) CDD Procedure is followed for all the joint loan account holders, while applying in joint.
- h) Circumstances in which, a customer is permitted to act on behalf of another person/ entity, is clearly spelt

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

out.

- i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India from time to time.
- j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation should not result in denial of AAVAS's services to general public, especially to those, who are financially or socially disadvantaged.

7. RISK MANAGEMENT

For Risk Management, AAVAS have a risk based approach which includes the following:

- Customers shall be categorised as low, medium and high risk category, based on the assessment and Risk perception of the HFC.
- The Risk categorisation has been undertaken based on parameters such as customer's identity, social/ financial status, nature of business activity and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

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 the KYC policy.

AAVAS shall include the Recommendations made by the Financial Action Task Force (FATF) the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment. Further, AAVAS briefly discuss Risk Categorisation of customers in its **Credit Policy**, approved by Board.

8. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

AAVAS shall undertake identification of customers in the following cases:

- (a) Commencement of an account-based relationship with the customer.
- (b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- (c) Selling Third Party Products as agents, selling their own products and any other product for more than rupees fifty thousand
- (d) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- (e) When a AAVAS has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- (f) AAVAS shall ensure that introduction is not to be sought while opening accounts.

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

- (a) Records or the information of the customer due diligence carried out by the third party is obtained within

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

two days from the third party or from the Central KYC Records Registry.

- (b) Adequate steps are taken by AAVAS to satisfy themselves 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.
- (c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act.
- (d) The third party shall not be based in a country or jurisdiction assessed as high risk.
- (e) The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, shall rest with the AAVAS.

9. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

Part- I CDD Procedure in case of individuals

AAVAS shall apply the following procedure while establishing an account based relationship with an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

- (a) the Aadhaar number where,
 - (i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - (ii) he decides to submit his Aadhaar number voluntarily to a AAVAS notified under first proviso to sub-section (1) of section 11A of the PML Act; or
 - (aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
 - (ab) 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; and
- (b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- (d) 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 AAVAS provided that where the customer has submitted,
 - i) Aadhaar number under clause (a) above to a AAVAS notified under first proviso to sub-section (1) of section 11A of the PML Act, AAVAS shall carry out authentication of the customer’s Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the AAVAS.
 - ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the AAVAS shall carry out offline verification.
 - iii) an equivalent e-document of any OVD, the AAVAS 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 Annex I.
 - iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the AAVAS shall carry out verification through digital KYC as specified under Annex I.

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

Provided that for a period not beyond such date as may be notified by the Government for a AAVAS, instead of carrying out digital KYC, the AAVAS pertaining to such class 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 (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, AAVAS 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 AAVAS and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. AAVAS shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the AAVAS and shall be available for supervisory review.

Explanation 1: AAVAS shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

- i. There must be a specific consent from the customer for authentication through OTP.
- ii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
- iii. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out.
- vi. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- vii. 21A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, AAVAS shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- viii. AAVAS shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

AAVAS may undertake live V-CIP, to be carried out by an official of the AAVAS, for establishment of

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

an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

- i. The official of the RE performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information of Aadhaar through Offline Verification.
- ii. AAVAS shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.
- iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India
- iv. The official of the AAVAS shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.
- v. The official of the AAVAS shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.
- vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.
- vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.
- viii. AAVAS shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. AAVAS shall carry out the liveness check in order to guard against spoofing and such other fraudulent manipulations.
- ix. To ensure security, robustness and end to end encryption, the REs shall carry out software and security audit and validation of the V-CIP application before rolling it out.
- x. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.
- xi. AAVAS shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.
- xii. AAVAS are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the RE.
- xiii. AAVAS shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

In case a person who desires to open an account is not able to produce documents, as specified in Section 16, AAVAS may at their discretion open accounts subject to the following conditions:

- (a) AAVAS shall obtain a self-attested photograph from the customer.
- (b) The designated officer of the AAVAS certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
- (c) The account shall remain operational initially for a period of twelve months, within which CDD as per Section 16 shall be carried out.
- (d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
- (e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
- (f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.
- (g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

KYC verification once done by one branch/office of the AAVAS shall be valid for transfer of the account to any other branch/office of the AAVAS, provided full KYC verification has already been done

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, identification information as mentioned under Section 14 in respect of the individual (proprietor) shall be obtained.

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.
- (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
- (c) Sales and income tax returns.
- (d) CST/VAT/GST certificate (provisional/ final).
- (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 AAVAS is satisfied that it is not possible to furnish two such documents, AAVAS may, at their discretion, accept only one of those documents as proof of business/activity.

Provided AAVAS undertake 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

For opening an account of a company, one certified copy of each of the following documents shall be obtained:

- (a) Certificate of incorporation;
- (b) Memorandum and Articles of Association;
- (c) Permanent Account Number 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;
- (e) One copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Numbers of Form 60 of the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

For opening an account of a partnership firm, one certified copy of each of the following documents shall be obtained:

- a) Registration certificate;
- b) Partnership deed;
- c) Permanent Account Number of the partnership firm;
- d) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Numbers of Form 60 of the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

For opening an account of a trust, one certified copy of each of the following documents shall be obtained:

- (a) Registration certificate;
- (b) Trust deed;
- (c) Permanent Account Number or Form No.60 of the trust;
- (d) one copy of an OVD containing details of identity and address, one recent photograph and Permanent

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

Account Numbers of Form 60 of the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf-

For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the following documents shall be obtained:

- (a) resolution of the managing body of such association or body of individuals;
- (b) Permanent Account Number or Form No.60 of the unincorporated association or a body of individuals;
- (c) power of attorney granted to transact on its behalf;
- (d) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Numbers of Form 60 of the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf identification information as mentioned under

Such information as may be required by the AAVAS to collectively establish the legal existence of such an association or body of individuals.

Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals', includes societies

For opening accounts of juridical persons not specifically covered in the earlier part, such as Government its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents shall be obtained:

- (a) Document showing name of the person authorised to act on behalf of the entity;
- (b) Aadhaar/PAN/ OVD for proof of identity and address in respect of the person holding an attorney to transact on its behalf and
- (c) Such documents as may be required by the HFC to establish the legal existence of such an entity/juridical person.

Part-IV CDD Measures for Identification of 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:

- (a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- (b) 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.

Part-V On-going Due Diligence Measures

AAVAS 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; and the source of funds. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- (a) 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.

(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

(c) High account turnover inconsistent with the size of the balance maintained.

(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts. The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

10. PERIODIC UPDATION

Periodic KYC updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

a) AAVAS shall carry out

i) PAN verification from the verification facility available with the issuing authority and

ii) Authentication, of Aadhaar Number already available with the AAVAS with the explicit consent of the customer in applicable cases.

iii) In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.

iv) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorised as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

v) In case of Legal entities, AAVAS shall review the documents sought at the time of opening of account and obtain fresh certified copies.

b) AAVAS may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD / Consent forwarded by the customer through mail/ post, etc., shall be acceptable.

c) AAVAS shall ensure to provide acknowledgment with date of having performed KYC updation.

d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

In case of existing customers, AAVAS 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 AAVAS 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. Provided that before temporarily ceasing operations for an account, the AAVAS shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, AAVAS shall include, in its

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

internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof 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 AAVAS gives in writing to the AAVAS that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, AAVAS 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.

Explanation – 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 by the AAVAS till such time the customer complies with the provisions of this Section.

Part VI - Enhanced and Simplified Due Diligence Procedure

Enhanced Due Diligence

Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):

AAVAS shall ensure that the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face-to-face customers.

Accounts of Politically Exposed Persons (PEPs):

(i) AAVAS shall have the option of establishing a relationship with PEPs provided that:

- (a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- (b) the identity of the person shall have been verified before accepting the PEP
- (c) The decision to open an account for a PEP is taken at senior level in accordance with the HFCs Customer Acceptance Policy;
- (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;
- (f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

(ii) These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

Customer's accounts opened by Professional Intermediaries:

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

- (a) Customer shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (b) HFCs 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.

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

(c) HFCs 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.

(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of HFC, 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 HFC shall look for the beneficial owners.

(e) HFCs 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.

(f) The ultimate responsibility for knowing the customer lies with the HFC.

Chapter VII- Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. AAVAS shall,

(a) maintain all necessary records of transactions between the AAVAS and the customer, both domestic and international, for at least five years from the date of transaction;

(b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transactions;

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

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

(f) 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;

(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Chapter VIII-Reporting Requirements to Financial Intelligence Unit - India

AAVAS shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

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

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide, prescribed/released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by AAVAS which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of AAVAS, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website <http://fiuindia.gov.in>.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. AAVAS shall not put any restriction on operations in the accounts where an STR has been filed. AAVAS shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Chapter IX-Requirements/obligations under International Agreements

Communications from International Agencies –

AAVAS shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do 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).

The details of the two lists are as under:

(a) The “ISIL (Da’esh) & Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>

(b) The “1988 Sanctions List”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl>

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other

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

jurisdictions/ entities from time to time shall also be taken note of.

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated March 14, 2019 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

(b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 55 a & b do not preclude AAVAS from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(b) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

Chapter-X OTHER MEASURES

Secrecy Obligations and Sharing of Information:

(i) AAVAS shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.

(ii) 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.

(ii) While considering the requests for data/information from Government and other agencies, AAVAS shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in transactions.

(iii) The exceptions to the said rule shall be as under:

- i. Where disclosure is under compulsion of law
- ii. Where there is a duty to the public to disclose,
- iii. the interest of bank requires disclosure and
- iv. Where the disclosure is made with the express or implied consent of the customer.

(e) NBFCs shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

Sharing KYC information with Central KYC Records Registry (CKYCR)

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

Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security



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

Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015. The 'live run' of the CKYCR would start with effect from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, AAVAS shall take the following steps:

(j) AAVAS shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

(ii) Operational Guidelines (version 1.1) for uploading the KYC data have been released by CERSAI. Further, 'Test Environment' has also been made available by CERSAI for the use of AAVAS.

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

Under FATCA and CRS, AAVAS shall adhere to the provisions of Income Tax Rule 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution
- Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to. HFCs shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H of Income Tax Rules.
- Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H of Income Tax Rules.
- Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
- Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

Introduction of New Technologies – Mobile Wallet/ Net Banking/ Mobile Banking/ RTGS/ NEFT/ ECS/ IMPS etc.

Adequate attention shall be paid by AAVAS to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

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 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process should be put in place.

(c) 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 of the HFC, regulation and

related issues should be ensured.

Selling Third party products:

AAVAS acting as agents while selling third party products shall comply with the applicable laws/regulations, including system capabilities for capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers.

Adherence to Know Your Customer (KYC) guidelines by AAVAS and persons authorised by AAVAS including brokers/agents etc.

- Persons authorized by AAVAS for collecting deposits and/ or selling loan related products, their brokers/ agents or the like, shall be fully compliant with the KYC guidelines applicable to AAVAS.
- All information shall be made available to the National Housing Bank to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by AAVAS including brokers/ agents etc. who are operating on their behalf.

AAVAS should ensure that the provisions of the PML Act, Rules framed thereunder and the Foreign Contribution (Regulation) Act, 2010, applicable, are adhered to strictly.

Where the AAVAS is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, the AAVAS may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

Annex I

Digital KYC Process

A. The AAVAS shall develop an application for digital KYC process 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 AAVAS.

B. The access of the Application shall be controlled by the AAVAS and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by AAVAS to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.

D. The AAVAS must 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 RE shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the AAVAS 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.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline



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

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.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. 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/eAadhaar 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.

I. 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 RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. 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 AAVAS. 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.

K. 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 AAVAS, 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.

L. The authorized officer of the AAVAS shall check and verify that:-

(i) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(ii) live photograph of the customer matches with the photo available in the document.; and

(iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the AAVAS 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.

Date of First Approval by Board: March 10, 2012

Date of last review by Board: February 02, 2023

Version : 1.1