

AML - KYC Policy

I. PREAMBLE:

This policy has been framed in accordance with the Reserve Bank of India (**RBI**) Master Direction – Know Your Customer (**KYC**) Direction, 2016, as amended from time to time and in terms of the provisions of Prevention of Money Laundering Act (**PMLA**), 2002 and rules and regulations made thereunder. In line with the said guidelines, this Policy details about the customer identification procedures while undertaking a transaction either by establishing an account-based relationship and monitor customer transactions. In view of the same, the Board of Directors of Avanse has adopted this policy framework on Anti Money Laundering (**AML**) – Know Your Customer (**KYC**) measures in line with the RBI guidelines.

II. BACKGROUND:

Money laundering refers to concealing or disguising the origin and ownership of the proceeds from criminal activity, including drug trafficking, public corruption, terrorism, fraud, human trafficking, and organized crime activities. Terrorist financing is the use of legally or illegally obtained funds to facilitate terrorist activities. Money laundering and terrorist financing may involve a wide variety of financial products, services, and transactions including lending and investment products, financing of equipment and other property that could be used to facilitate terrorism and other criminal activity.

Generally, the money laundering process involves three (3) stages: placement, layering and integration. As illegal funds move from the placement stage through the integration stage, they become increasingly harder to detect and trace back to the illegal source.

- a. **Placement** is the point where illegal funds first enter the financial system.
- b. **Layering** After illegal funds have entered the financial system, layers are created by closing and opening accounts, purchasing and selling various financial products, transferring funds among financial institutions and across national borders. The criminal's goal is to create layers of transactions to make it difficult to trace the illegal origin of the funds.
- c. **Integration** occurs when the criminal believes that there are sufficient numbers of layers hiding the origin of the illegal funds to safely invest the funds or apply them towards purchasing valuable property in the legitimate economy.

To prevent money-laundering in India and to provide for confiscation of property derived from, or involved in, money-laundering and related matters, the Parliament of India enacted the PMLA, as amended from time to time. Further, necessary Notifications / Rules under the said Act have been published and amended by the Ministry of Finance, the Government of India.

As per the PMLA, the offence of Money Laundering is defined as:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."

Punishment for Money Laundering is laid down as “whoever commits the offense of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three (3) years but may extend to ten (10) years.”

The PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime. Given the aforesaid background, this AML - KYC Policy shall broadly achieve the following purposes:

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

The Policy will be applicable to all branches/offices and the employees of Avanse and is to be read in conjunction with related operational guidelines, if any, issued from time to time.

III. **DEFINITIONS:**

1. Unique Identification Authority of India (UIDAI) / Aadhaar number:

It means and includes Aadhaar card which entails an identification number issued to an individual by UIDAI on receipt of the demographic and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter called as ‘Aadhaar Act’), as amended from time to time.

Explanation 1: In terms of the Aadhaar Act, every resident shall be eligible to obtain an Aadhaar / UIDAI number.

Explanation 2: Aadhaar will be the document for proof of identity and address.

2. Aadhaar Authentication:

As defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic or biometric information of an individual is voluntarily submitted by him/her to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

3. Beneficial Owner:

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

Explanation –

1. “Controlling ownership interest” means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
2. “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

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

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

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

- (iv) Where the **customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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.

4. Biometric information:

As defined in the Section 2(g) of the Aadhaar Act, means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by Aadhaar regulations.

5. Central Identities Data Repository (CIDR):

As defined in Section 2(h) of the Aadhaar Act, means a centralized database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.

6. Certified copy:

Obtaining a copy of KYC document (includes Pol and PoA) from a Customer by Avanse, where offline verification cannot be carried out, and comparing such copy with the original of the KYC document so produced by the customer and recording the same on the copy by the authorised officer of Avanse. In common parlance this is referred as 'Original Seen and Verified' - OSV procedure.

7. Central KYC Records Registry (CKYCR):

An entity, authorized by the Government through an official gazette notification to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

8. Customer:

- (i) A person or entity that maintains an account and/or has a business relationship with Avanse;
- (ii) A person who is engaged in a financial transaction or activity with Avanse and includes a person on whose behalf the person who is engaged in the transaction or activity.
- (iii) One, on whose behalf the account is maintained (i.e. the beneficial owner)
- (iv) Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

Any other person or entity connected with a financial transaction which can pose significant reputation or other risks to Avanse, say a wire transfer or issue of high value demand draft as a single transaction.

9. Customer Due Diligence (CDD): Identifying and verifying the customer and the beneficial owner.

10. Digital KYC means capturing the live photo of the client and OVD or the proof of possession of Aadhaar, (i.e. 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 authorized officer of the reporting entity as per guidelines detailed in **Annexure V**).

11. Digital Signature means authentication of any electronic record by a subscriber by use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. Any person by the use of a 'public key' of the subscriber can verify such electronic records.

Explanation – "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record.

12. Demographic information:

As defined in Section 2(k) of the Aadhaar Act, includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.

13. 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 client as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

14. Know Your Client (KYC) Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.

15. Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

- Currently, the process of Offline Verification as per UIDAI website includes following:
 - i. It is an alternate means to submit Aadhaar as a KYC Proof.
 - ii. It is carried out through UIDAI site, wherein the Customer can download XML Zip file containing his/ her personal and demographic information.
 - iii. The XML Zip file is digitally signed by UIDAI, which is a secured shareable document and is shared with Avanse as a KYC proof along with the four (4) digit share code.
 - iv. As such, sharing of said XML Zip file completes the process of submitting Aadhaar as a KYC proof, without the need to mention Aadhaar number.

16. Officially valid document (OVD) – means

- (i) Passport,
- (ii) Driving license,
- (iii) Voter ID / Election ID card,
- (iv) Job card issued by NREGA duly signed by an officer of the State Government
- (v) Letter issued by the National Population Register containing details of name and address,
- (vi) Proof of possession of Aadhaar number to be obtained after express consent of the Customer, as defined below:
 - a. Virtual Identity (ID) generated from the UIDAI by the Customer, verifying personal and demographic information by Avanse with UIDAI database.
 - b. Offline Verification of Aadhaar as per Aadhaar regulations.
 - c. Aadhaar Card (to be obtained after Customer redacts or blackouts 1st 8 digits of the Aadhaar number)
- (vii) Equivalent e-document containing the details of the identity and address of the Customer, for which Avanse shall verify the digital signature of such e-document submitted.

Provided that,

- a. where the customer voluntarily submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the UIDAI.
- b. where the OVD furnished by the customer does not have the 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:-
 - i. Utility bill, which is not more than two (2) 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 PSUs, if they contain address;
 - iv. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation;
 - v. For the above purpose, 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.

17. Person - means and includes:

- (i) an Individual
- (ii) A Hindu Undivided Family,
- (iii) A Company
- (iv) A Firm
- (v) an association of persons or a body of individuals, whether incorporated or not,
- (vi) every artificial juridical person, not falling within any one of the above persons (i to v), and
- (vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

18. Politically Exposed Persons (PEPs) - are individuals who are or have been entrusted with prominent public functions in India and/or foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/police/judicial/military officers, senior executives of state- owned corporations (Chief Executive/Directors and above levels), important political party officials, etc.

19. Senior Management - for the purpose of KYC compliance shall include Designated Director, Head of Credit, Head of Risk, Business Heads, Key Managerial Persons, Compliance Officer, Principal Officer (PO) and his/her supervisor.

20. Suspicious Transaction means a "transaction" including an attempted transaction, whether or not made in cash, which, to a person acting in goodfaith:

- (i) 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
- (ii) appears to be made in circumstances of unusual or unjustified complexity; or
- (iii) appears to not have economic rationale or bona-fide purpose; or
- (iv) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

21. Video based Customer Identification Process (V-CIP): V-CIP is a method of customer identification by an official 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 (detailed in **Annexure IV**).

IV. CUSTOMER ACCEPTANCE POLICY (“CAP”)

The guidelines in respect of the customer relationship with Avanse broadly are detailed below:

- i. No account is to be opened in anonymous or fictitious/benami name(s)/entity (ies).
- ii. Accept customers only after verifying their identity, as per CDD Procedures defined herein and shall be followed for all the joint account holders / co-applicants (including guarantors) as well, while opening a joint account. In case where a customer is other than a natural person, the identification of Beneficial Owner (**BO**) shall be carried out by obtaining a declaration from such customer, wherever applicable and reviewing the same.
- iii. Necessary checks before opening a new account are to be ensured so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious and reported.
- iv. In relation to digital on-boarding, where no face to face interaction is possible with the Customer, Avanse through its authorised official may undertake V-CIP (**Annexure IV**) procedure for establishment of an account based relationship with an individual customer, after obtaining his/ her informed consent.
- v. Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization.
- vi. Appropriate Enhanced Due Diligence (EDD) measures (refer **Annexure I**) shall be adopted for high risk customers from AML- KYC perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are PEPs and their family members/close relatives.
- vii. In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures (refer **Annexure I**) shall be adopted.
- viii. Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with PMLA and RBI guidelines/instructions are indicated in **Annexure II** to this Policy. The information collected from the Customers shall be kept confidential.
- ix. Not to open an account or close an existing account (except as provided in this Policy), where CDD measures as defined in this Policy could not be applied, due to non - cooperation of the customer or non - reliability of the data/ information furnished to Avanse. Suitable built – in safeguards shall be provided to avoid any harassment to Customers.
- x. Implementation of CAP should not become too restrictive and result in denial of Avanse services to general public, especially to those who are financially or socially disadvantaged.
- xi. The decision to open an account for PEP should be taken at a senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
- xii. Circumstances, in which a customer is permitted to act on behalf of another person/entity shall be clearly spelt out in conformity with the established law and practice and shall be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity or beneficial owner.
- xiii. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified.
- xiv. 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 RBI.
- xv. Avanse shall seek only such information from the customer which is relevant to the risk category and is not intrusive. Any other information from the customer should be sought separately with his/her consent and after opening the account.
- xvi. Avanse shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level. If an existing KYC compliant customer of Avanse desires to open another account with it, there shall be no need for a fresh CDD exercise.
- xvii. Decision-making functions of determining compliance with KYC norms shall not be outsourced.

V. RISK MANAGEMENT

For Risk Management, Avanse will 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 Avanse
- (ii) Risk categorization shall be 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.

Avanse shall prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy. The customer profile shall contain the information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by Avanse. These requirements may be moderated according to the risk perception.

(i) High Risk – (Category A):

High risk customers typically will include:

- a. Individuals and entities listed or identified in – various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267, schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.;
- b. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.
- c. Non - resident Customers (excluding applicants for retail education loans).
- d. High net worth individuals without an occupation track record of more than 3 years.
- e. Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations, having business or charitable purpose other than Education.
- f. Firms with sleeping partners.
- g. Politically exposed persons (PEPs) of Indian/ foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- h. Customers with dubious reputation as per public information available or commercially available watch lists.
- i. Gambling/gaming including “Junket Operators” arranging gambling tours.
- j. Jewelers and Bullion Dealers.
- k. Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
- l. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries).
- m. Customers that may appear to be Multi-level marketing companies etc.
- n. Any borrower/co-borrower working in a country identified as high risk.

(ii) Medium Risk – (Category B):

Medium risk customers typically will include:

- a. Trust, charitable organizations, non govt. organization (NGO), organizations receiving donations (i.e. who are running education institutions).
- b. Salaried applicant with variable income/ unstructured income receiving salary in cheque.
- c. Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialing (IDD) call service.
- d. Self - employed professionals other than HNIs (excluding applicants for retail education loans).
- e. High net worth individuals with occupation track record of more than 3 years.
- f. One of more borrowers' resident outside India (excluding student going abroad to study).
- g. Companies having close family shareholding or beneficial ownership.
- h. None face to face to customers (Refer **Annexure I**).

(iii) Low Risk – (Category C):

Low risk customers typically will include:

- a. Salaried employees with well-defined salary structures
- b. People working with government owned companies, regulators and statutory bodies, etc.
- c. People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
- d. People working with Public Sector Units.
- e. People working with reputed Public Limited Companies and Multinational Companies.
- f. All borrowers resident in India (including student going abroad to study).
- g. Low risk individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and all other person not covered under above two categories.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, Avanse will undertake EDD measures as specified in **Annexure I**.

VI. CUSTOMER IDENTIFICATION PROCEDURES ("CIP")

1. Avanse 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;
 - iii. Selling their own products, selling third party products as agents and any other product for more than Rs.50, 000/-.
 - iv. Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50, 000/-, whether conducted as a single transaction or several transactions that appear to be connected.
 - v. When Avanse 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 Rs.50,000/-.
2. Avanse will obtain Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B and the same shall be verified from the verification facility available with the issuing authority like from NSDL. Form 60 shall be obtained from persons who do not have PAN.
3. Avanse will verify the digital signature as per the provisions of the Information Technology Act, 2000 for the equivalent e-document obtained from customer.
4. For the customers that are legal person or entities, Avanse will verify the legal status for the legal person/ entity through proper and relevant documents;
5. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Avanse , at its discretion may at its option, rely on CDD done by a third party, subject to the following conditions:
 - i. Records or the information of the CDD carried out by the third party is obtained within two (2) days

- from the third party or from the Central KYCrecords registry.
- ii. Adequate steps are taken by Avanse to satisfy that copies of identification data and other relevant documentation relating to CDD shall be made available from the third party upon request without delay.
- iii. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with CDD and record-keeping requirements in line with the requirements and obligations under the PMLA Act;
- iv. The third party shall not be based in a country/ jurisdiction assessed as high risk;
- v. The ultimate responsibility for CDD and undertaking EDD measures (as per Annexure I), as applicable, will be with Avanse.
- 6. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for cross selling or other purpose, except with the express consent from the customer.
- 7. The Company will have monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

Note: Avanse will capture the KYC information for sharing with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, under the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company will upload the KYC data pertaining to all types of prescribed accounts with CKYCR, as and when required, in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and guidelines prescribed by CKYC and CERSAI in this regard. Once the Customer's data is uploaded on the CYCKR, a unique KYC identifier number is generated that is assigned to the customer by the CKYCR, or where the Customer's KYC identifier is already available in CKYCR database, the same shall be updated / validated as the case may be.

- 8. KYC verification once done by one branch/office of Avanse shall be valid for transfer of the account to any other branch/office of Avanse, provided full KYC verification has already been done for the concerned account and the same is not due for periodic update.
- 9. While undertaking customer identification, the Company will ensure that:
 - i. The customers shall not be required to furnish an additional OVD, if the OVD submitted for KYC contains proof of identity as well as proof of address e.g. Passport. An indicative list of the nature and type of documents/information that may be relied upon for customer due diligence / identification is given in **Annexure II**.
 - ii. In case of 'change of address' requested by a customer, he/she should provide a fresh KYC / PoA in support of new address as per **Annexure II**.
 - iii. Such other documents pertaining to the nature of business or financial status specified by Avanse.
 - iv. Enhanced Due diligence measures are indicated in **Annexure I**.

VII. Periodic Updating of KYC data:

Avanse shall periodically update Customer's KYC information / documents after the transaction is entered. The periodicity of updating of Customer's KYC data shall be carried out once in 10 years for low risk customers, once in every 8 years for medium risk customers, and once in 2 years for high risk categories, as per the following procedure:

Avanse shall carry out –

- i. PAN verification from the verification facility available with the issuing authority.
- ii. Authentication, of Aadhaar Number already available with Avanse 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 as per **Annexure II**.

- iv. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized 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, Avanse shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- vi. Avanse 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.
- vii. Avanse shall ensure to provide acknowledgment to the customer with date of having performed KYC updation.
- viii. As regards to the customers of the Education Institutional business of the Company, any customer sanctioned more than Rs. 1 crore loan and customers tagged as 'medium risk' (as per para V above), additional checks (i.e. CDD measures) for PEP identification and negative market news around any of the borrower / co-borrower shall also be carried out. Basis the results of these checks, re-classification as per para V above and other CDD and/or EDD measures will be undertaken.

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

VIII. SIMPLIFIED PROCEDURE:

In case a person who desires to open an account is not able to produce identification information as per Annexure II, Avanse may at their discretion open accounts subject to the following conditions:

- (a) Obtain a self-attested photograph from the customer.
- (b) Avanse 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 12 (twelve) months, within which the customer has to furnish identification information as per Annexure II.
- (d) The total credit in all the accounts taken together shall not exceed Rs. 1,00,000/- in a year.
- (e) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (e) above are breached by him.
- (f) The customer shall be notified when the total credit in a year reaches Rs. 80,000/- 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 (e) above.

IX. MONITORING OF TRANSACTIONS:

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. Avanse shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Avanse may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Higher risk accounts shall be subjected to intense monitoring.

Avanse shall set key indicators for such accounts basis the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. The extent of monitoring shall be aligned with the risk category of the customer. Avanse shall carry out the periodic review of risk categorization of transactions/customer's accounts and the need

for applying EDD measures at a periodicity of not less than once in six (6) months.

X. TRAINING PROGRAMME:

- i. Avanse shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for frontline staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.
- ii. Authorised officials undertaking V-CIP process shall be adequately trained from time to time.

XI. INTERNAL CONTROL SYSTEM:

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Avanse's own policies and procedures, including legal and regulatory requirements. The Management under the supervision of Board shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals till closure of audit findings.

Further, Avanse shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

XII. RECORD KEEPING:

- Maintenance of records of transactions

Avanse shall maintain proper record of the transactions (including the records of the Customer who are on boarded through V-CIP) as required under Section 12 of the PMLA read with Rules 3 of the PML Rules as mentioned below:

- (i) All cash transactions of the value of more than Rs. ten (10) lacs, though by policy the Company does not accept cash deposits in foreign currency.
- (ii) All series of cash transactions integrally connected to each other which have been valued below Rs. ten (10) lacs where such series of transactions have taken place within a month.
- (iii) All transactions involving receipts by non-profit organizations of rupees ten (10) lakhs or its equivalent in foreign currency.
- (iv) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions;
- (v) records pertaining to identification of the customer and his/her address; and
- (vi) All suspicious transactions whether or not made in cash and in manner as mentioned in the Rule framed by the Government of India under PMLA.

An Illustrative List of suspicious transaction pertaining to financial services is given in **Annexure III**.

- Records to contain the specified information

The Records referred to above in Rule 3 of PMLA Rules to contain the following information:

- a. the nature of the transactions;
- b. the amount of the transaction and the currency in which it was denominated;
- c. the date on which the transaction was conducted; and
- d. the parties to the transaction.

- Maintenance and preservation of records

Section 12 of PMLA requires Avanse to maintain records as under:

- e. records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of five (5) years from the date of transactions between the clients and Avanse.
- f. records of the identity of all clients of Avanse is required to be maintained for a period of five (5) years from the date of cessation of transactions between the clients and Avanse.

Avanse shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or as/ when requested by the competent authorities.

XIII. APPOINTMENT OF PRINCIPAL OFFICER:

Avanse shall designate a senior employee as 'Principal Officer' (PO) who shall be located at the Head/Corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

XIV. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA:

In accordance with the requirements under PMLA, the Principal Officer of Avanse will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

- a) Cash Transaction Report (CTR) - If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.
- b) Counterfeit Currency Report (CCR) - All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.
- c) Suspicious Transactions Reporting (STR) - The Company will endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to FIU-IND.

Avanse will file the Suspicious Transaction Report (STR) to FIU-IND within seven (7) days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, Avanse will not put any restriction on operations in the accounts where an STR has been filed. An indicative list of suspicious transactions is enclosed as **Annexure III**.

The employees of Avanse shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

XV. APPOINTMENT OF DESIGNATED DIRECTOR:

The Board of Directors shall nominate a “Designated Director” to ensure compliance with the obligations prescribed by the PMLA and the Rules there under. The “Designated Director” can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the “Designated Director”. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

XVI. GENERAL:

1. Closure of Accounts/Termination of Financing/Business Relationship

Where Avanse is unable to apply appropriate KYC measures due to non - furnishing of information and/or non-cooperation by the customer, Avanse shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of either Chief Executive Officer or Designated Director or Chief Risk Officer or Principal Officer of the Company.

2. KYC for the Existing Accounts:

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions with existing customers would be continuously monitored for any unusual pattern in the operation of the accounts.

3. Changes to AML- KYC Policy.

In case of issue of any guidelines, circulars and regulations by RBI/FIU/PMLA amending the existing AML – KYC provisions applicable to Avanse, which warrants changes to this policy, the Principal Officer jointly with the Designated Director will be authorized to circulate the said amendments among the employees/ branches for its due implementation and shall form part and parcel of this policy. In this regard, the Principal Officer jointly with the Designated Director shall ensure that the updated policy aligned with the applicable regulations is placed before the Board of Directors on an annual basis for its perusal, review and ratification thereto. It is hereby clarified any changes in line with business (non – regulatory) requirements shall require prior approval of the Board before its implementation / circulation.

Enhanced Due Diligence (EDD) measures

1. Accounts of PEPs

- 1.1 Branch/office shall gather sufficient information on any PEP customer intending to establish a relationship and check all the information available in the public domain.
- 1.2 Branch/office shall verify the identity of the PEP and seek information about the sources of funds before accepting said PEP as a Customer.
- 1.3 The decision to provide any loan to the PEP customer shall be taken as per applicable Compliance, Risk & Underwriting policies of Avanse, with ongoing monitoring.
- 1.4 The above instructions are also applicable where the PEP is a Beneficial Owner.

2. Accounts of non-face-to-face customers

- 2.1 In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk.
- 2.2 Avanse shall ensure that the first payment is to be effected through the customer's KYC- complied account with another Regulated Entity, for EDD of non-face to face customers.

3. Trust/Nominee or Fiduciary Accounts

Branch/offices shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, they shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

Avanse shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', branches shall take steps to verify the founder managers/ directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

4. Accounts of companies and firms

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with NBFCs. Branch/ office may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it shall not be necessary to identify all the shareholders.

Annexure II

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers

<p>INDIVIDUALS (includes Beneficial owner, Authorized Signatory, Power of Attorney)</p>	<p>I. Proofs of Identity (Pol):-</p> <ol style="list-style-type: none"> *Pan Card/Form 60 (OVD) *One (1) recent colour photograph <p>*Mandatory documents</p> <p>Note: Additional / Optional documents to be obtained along with Form 60:</p> <ol style="list-style-type: none"> Passport (OVD) Voter' s Identity Card (OVD) Driving License(OVD) Aadhaar Card (OVD) – to be collected after masking 1st 8 digits of the Aadhaar number Alternate means to Aadhaar Card <ul style="list-style-type: none"> Virtual ID in lieu of Aadhaar number. Offline Verification. Letter issued by the National Population Register containing details of name & address (OVD) Job card issued by NREGA duly signed by an Officer of State Government (OVD) Equivalent e-document containing the details of the identity (OVD) <p>II. Proof of address (PoA):-</p> <ol style="list-style-type: none"> Passport (OVD) Driving License (OVD) Voter' s Identity Card (OVD) Aadhaar Card (OVD) Job card issued by NREGA duly signed by an Officer of State Government (OVD) Letter issued by the National Population Register containing details of name & address(OVD) Equivalent e-document containing the details of address (OVD). <p>Note: Additional / Optional documents to be obtained in case the address mentioned in the OVD is different from the current/correspondence address:</p> <ol style="list-style-type: none"> Registered Leave & License Agreement or Rent Agreement having the validity as on the date of entering into a relationship with the company. Pension or family Pension payment orders (PPOs) issued to retired employees by Government Departments or PSUs, if they contain address. A person not having an address proof in his/her own name may provide an address proof (as accepted by the company) of any close relative (e.g. Spouse, son, daughter, parents) supported by a document establishing their relationship (e.g. Pan Card, Passport, Birth Certificate. Etc.,) supported with a declaration that the said customer is residing with the relative whose address proof is being provided to the company. Pan card intimation/ allotment letter. For students residing in a Hostel, Hostel room allotment letter/letter from college office. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India. Property or Municipal Tax Paid Receipt not more than 3 months old. Bank Account or Post Office savings bank account Statement.
--	--

	<p>ix. Telephone bill / Postpaid Mobile phone bill / Electricity bill / Water Bill / Piped Gas bill not more than 2 months old.</p> <p>x. Ration Card.</p> <p>xi. Copy of agreement to sale / sale deed.</p> <p>xii. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, Public Sector Undertakings, scheduled commercial banks, financial institutions and listed companies.</p> <p>III. SIGNATURE PROOF:- (signature to match with self - attestation, application form and loan documents)</p> <ol style="list-style-type: none"> 1). Banker's signature verification/authentication 2). Passport Copy 3). PAN Card 4). Driving license with photograph and signature 5). Clearance of processing fees cheque – concerned officer has to verify signature on application form with processing feescheque.
PRIVATE / PUBLIC LIMITED COMPANY / LLPS	<p>Mandatory documents – One (1) certified copy of each of the following documents [or the equivalent e-documents thereof] needs to be obtained:</p> <ol style="list-style-type: none"> 1) Certificate of incorporation 2) Memorandum & Articles of Association 3) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf. 4) Certified copies of PAN and OVD (for PoI and PoA purpose), and Photograph) in respect of managers, officers or employees holding an attorney to transact on its behalf. 5) *PAN card <p>*Note: PAN or form 60 in lieu of PAN and PoA of the Directors, KMPs, Partners, or persons holding an attorney to transact the business on behalf of entity.</p> <p>Additional / Optional documents:</p> <ol style="list-style-type: none"> 6) Certificate / registration document issued by Sales Tax / GST / Professional Tax authorities 7) Copy of the utility bill (not more than two months old)/ Copy of PAN allotment letter for PoA 8) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document.

<p>PARTNERSHIP FIRM</p>	<p>Mandatory documents – One (1) certified copy of each of the following documents [or the equivalent e-documents thereof] needs to be obtained: 1). Registration certificate, if registered 2). *PAN card 3). Partnership deed 4) Certified copies of PAN and OVD (for Pol and PoA purpose), and Photograph in respect of the person holding an attorney to transact on its behalf *Note: PAN or form 60 in lieu of PAN and PoA of the Partners, or persons holding an attorney to transact the business on behalf of entity.</p> <p>Additional / Optional documents: 5). Certificate / registration document issued by Sales Tax / GST / Professional Tax authorities 6). Copy of the utility bill (not more than two months old)/ Copy of PAN allotment letter for PoA). IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document.</p>
<p>SOLE PROPRIETORSHIP FIRM</p>	<p>Mandatory documents –</p> <ol style="list-style-type: none"> 1) Certified copies of each of PAN and OVD (for Pol and PoA purpose), and Photograph of the Individual (i.e. Proprietor). 2) In addition to the above, certified copies of any two (2) of the following documents [or the equivalent e-documents thereof] shall also be obtained: <ol style="list-style-type: none"> i. Registration certificate ii. Certificate/ licence issued by the municipal authorities under Shop and Establishment Act. iii. Sales and income tax returns (provisional/final). iv. CST/VAT/ GST certificate v. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. vii. 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. viii. Utility bills such as electricity, water, and landline telephone bills.

<p style="text-align: center;">TRUST</p>	<p>Mandatory documents – One (1) certified copy of each of the following documents [or the equivalent e-documents thereof] needs to be obtained: (a) Registration certificate (b) Trust deed) Certified copies of PAN and OVD (for Pol and PoA purpose), and Photograph of Trustees and/or other person holding a power of attorney to transact on its behalf) *PAN card *Note: PAN or form 60 in lieu of PAN and PoA of the Trustees or persons holding an attorney to transact the business on behalf of entity. Additional / Optional documents: 1. Certificate / registration document issued by Sales Tax / GST / Professional Tax authorities 2. Copy of the utility bill (not more than two months old)/ Copy of PAN allotment letter for PoA</p>
<p style="text-align: center;">Unincorporated associations 1. Association of Persons (AOP) 2. Body of Individuals (BOI)</p> <p><i><u>Explanation 1:</u> Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.</i></p> <p><i><u>Explanation 2:</u> Term 'body of individuals' includes societies.</i></p>	<p>Mandatory documents – One (1) certified copy of each of the following documents [or the equivalent e-documents thereof] needs to be obtained: (a) resolution of the managing body of such association or body of individuals; (b) power of attorney granted to transact on its behalf; (c) Certified copies of PAN and OVD (for Pol and PoA purpose), and Photograph in respect of the person holding an attorney to transact on its behalf and d) Any such information as may be required by AFSL to collectively establish the legal existence of such an association or body of individuals. (f) *PAN card *Note: PAN or form 60 in lieu of PAN and PoA of the Partners, or persons holding an attorney to transact the business on behalf of entity. Additional / Optional documents: 1). Certificate / registration document issued by Sales Tax / GST / Professional Tax authorities</p>
<p>Juridical persons not specifically covered in the earlier part, such as Government or its Departments, Societies, Universities and Local bodies like Village Panchayats</p>	<p>Mandatory documents – One (1) certified copy of each of the following documents [or the equivalent e-documents thereof] needs to be obtained: 1. Document showing name of the person authorised to act on behalf of the entity i.e. Authority Letter, or Power of Attorney; 2. Certified copies of PAN and OVD (for Pol and PoA purpose), and Photograph in respect of the person holding an attorney / authority to transact on its behalf 3. Such documents as may be required by Avanse to establish the legal existence of such an entity/juridical person. Additional / Optional documents: 4. Certificate / registration document issued by Sales Tax / GST / Professional Tax authorities 5. Copy of the utility bill (not more than two months old) / Copy of PAN allotment letter for PoA</p>

Annexure III

A. Broad categories of reason for suspicion and examples of suspicious transactions for Non Banking Financial Companies are indicated as under:

1. Identity of client

- False identification documents.
- Identification documents which could not be verified within reasonable time.
- Accounts opened with names very close to other established business entities.

2. Background of client

- Suspicious background or links with known criminals.

3. Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale.

4. Activity in accounts

- Unusual activity compared with past transactions.

5. Nature of transactions

- Unusual or unjustified complexity.
- Involves proceeds of an criminal / illegal activity, regardless of the value involved
- No economic rationale or bonafide purpose.
- Frequent purchases of drafts or other negotiable instruments with cash.
- Nature of transactions inconsistent with what would be expected from declared business.
- Reasonable ground of suspicion that it may involve financing of activities relating to terrorism and/or account holder / beneficial owner linked or related to terrorist, terrorist organization or those who finance or attempt to finance terrorist activities.

6. Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
- Value inconsistent with the client's apparent financial standing.

B. Illustrative list of Suspicious Transactions

- Reluctant to part with information, data and documents.
- Submission of false documents, purpose of loan and detail of accounts.
- Reluctance to furnish details of source of funds of initial contribution.
- Reluctance to meet in person, representing through power of attorney.
- Approaching a distant branch away from own address.
- Maintaining multiple accounts without explanation.
- Payment of initial contribution through unrelated third party account.
- Suggesting dubious means for sanction of loan.
- Where transactions do not make economic sense.
- Where doubt about beneficial ownership.
- Encashment of loan through a fictitious bank account.
- Sale consideration quoted higher or lower than prevailing area prices.
- Request for payment in favor of third party with no relation to transaction.
- Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent.
- Frequent request for change of address.
- Overpayment of installments with a request to refund the overpaid amount.
- Approvals/sanctions from authorities are proved to be fake.
- Overpayment of installments with a request to refund the overpaid amount.

V – CIP Guidelines

V-CIP process as detailed below shall be undertaken where Offline Aadhaar Verification for Customer on – boarding is possible:

1. The V-CIP customer on-boarding process shall only be triggered from the domain of Avanse. IT application developed for this purpose, shall be accessed through login id and password or Live OTP/ Time OTP controlled mechanism by authorized officials of Avanse. For this purpose, a link to be provided to the Customer which shall be triggered / made available for video interaction with the authorized officials of Avanse.
2. The said application should envisage seamless, real time, secured, end to end encryption of audio – visual interaction between the Customer and the authorized official of Avanse, so as to assess/ verify identity of the Customer beyond doubt. Further, the application shall also enable liveness check of the Customer in order to guard against spoofing and fraudulent manipulations. Towards this purpose, Avanse official shall ensure that the sequence and/ or type of questions during the video interactions are varied in order to establish that the interactions are real time and not pre – recorded.
3. In order to ensure robustness of the information security of the application, Avanse shall carry out software and security audit and validation of the V-CIP application before the same goes live.
4. The application shall have the functionality of capturing the live Geo tagging (with Latitude & Longitude) of the Customer's location in order to ensure that the Customer is physically present in India.
5. V-CIP process and application shall enable capturing of clear image of PAN card displayed by the Customer during the process, except in cases where e-PAN is provided. The said PAN details shall be verified from the database of the issuing authority. Further, as regards to obtaining KYC of the Customer as 'proof of address', only offline verification of Aadhaar of the Customer shall be carried out in line with UIDAI directions, and the XML / QR files should not be more than three (3) days old from date of Video.
6. Avanse's official shall ensure that the photograph and the demographic/personal information of the customer in the Aadhaar/PAN matches with the details provided by the customer in the loan application. Towards this purpose, Avanse in line with the best industry practices shall take assistance of the latest available technology like Optical Character Recognition ('OCR'), including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer is maintained throughout. However, the responsibility of customer identification shall always rest with Avanse.
7. Logs of Video interaction along with date & time stamp and credentials of the official of Avanse who have undertaken respective V-CIP customer on-boarding shall be preserved from the date of loan sanction and 5 years after foreclosure.
8. Concurrent audit is mandatory before any loan account is sanctioned, which will be an ongoing exercise for all customers on-boarded through V-CIP. The audit can be conducted by the employee of Avanse or through external party possessing relevant qualification / experience.

Digital KYC process

Digital KYC process as detailed below shall be undertaken where **Offline Aadhaar Verification for Customer on – boarding is not possible:**

1. A secured application which can be accessed only through login id and password or Live OTP/ Time OTP controlled mechanism by authorized officials of Avanse shall be developed and made available at Customer touch points for Individual Customer Digital KYC on boarding.
2. Customer shall visit the location of Avanse's authorized official or vice- versa along with his/ her original OVD.
3. The said application shall enable that customer's live photo is only captured and no printed/video graphed photo is captured, such that background of the photo should be in white and no other person shall come into frame while capturing the said photo. The said live photo shall be embedded in the Customer Application Form (CAF) along with water marking in readable form with CAF number, GPS coordinates, authorized official's name, employee code, date (DD:MM:YYYY) & Time stamp (HH:MM:SS) on the CAF.
4. Further, the live photo of the original OVD incl. Aadhaar card shall be placed horizontally by the Customer and photo of the same shall be captured vertically from above with water marking in readable form, as aforesaid. There should be no tilt in the mobile device while capturing the live photo of the original documents. Further, the live photo of the client and his original documents shall be captured in proper light so that they are clearly visible.
5. All entries in the CAF shall be filled as per the documents and information furnished by the customer. In documents where Quick Response (QR) code is available, such details can be auto - populated by scanning the QR code instead of manually filling the details.
6. Once the aforesaid process is completed, an OTP message containing the text "Please verify the details filled in form before sharing OTP" shall be sent to the customer's own mobile number. Upon successful OTP validation, 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 same shall be clearly mentioned in CAF. In any case, the mobile number of Avanse's authorized officer shall not be used for client signature, which shall also be cross – verified before loan sanction.
7. The authorized officer shall check and verify that:
 - i. Information available in the picture of OVD of the Customer including live photo matches with the information in CAF, and
 - ii. all of the necessary details in CAF including mandatory fields are filled properly.
8. The authorized officer shall provide a declaration about capturing of the live photo and OVD of the Customer. For this purpose, the authorized official shall verify OTP received on his/her mobile number registered with Avanse. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photo of the authorized official shall also be captured with the said declaration.
9. On successful verification, the CAF shall be digitally signed by the authorized officer who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in Loan Management System (LMS) of Avanse.
10. Subsequent to all the aforesaid activities, the said application shall give information about the completion of the process and submission of activation request to the Loan Management System (LMS) of Avanse. Furthermore, LMS shall generate the reference-id number of the process and an email/SMS confirming completion of the process along with reference id shall be sent to the customer and the authorized officer.