GETGROWTH CAPITAL PRIVATE LIMITED

KYC & AML POLICY

DOCUMENT OWNER & VERSION CONTROL

Policy Name	KYC & AML Policy
Issue and Effective Date	March 6, 2023
Periodicity of Review	Annually or as recommended by the Board of Directors
Approving Authority	Board of Directors

Particulars	**Creation/ Review**	**Approval Date**
Version 1.0	Creation	March 6, 2023

1. PREAMBLE

The Board of Directors (the "**Board**") of GetGrowth Capital Private Limited (the "**Company**" or "**GetGrowth**"), has adopted the following policy regarding salient features of Know Your Customer ("**KYC**") and Anti-Money Laundering (''**AML**'') norms together referred to as **"Policy"** for GetGrowth Capital Private Limited as prescribed by Reserve Bank of India ("**RBI**").

The policy has been framed in accordance with "**Master Direction - Know Your Customer (KYC) Directions, 2016**" issued by the RBI vide Circular RBI/DBR/2015-16/18 DBR.AML.BC. No.81/14.01. dated February 25, 2016 and Circular RBI/2016-17/183 DBR.AML.BC.48/14.01.01/2016-17 dated December 15, 2016 and "**Master Circular – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards (AML) -'Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules notified thereunder**" vide Circular RBI/2015-16/108 DNBR (PD) CC No. 051/03.10.119/2015-16 dated July 1, 2015. Further, the policy is drafted in accordance with the changes carried out in the "Master Direction - Know Your Customer (KYC) Directions, 2016" issued vide Circular RBI/2019-20/221 DOR.AML.BC. No.66/14.01.001/2019-20 dated April 20, 2020 and necessary applicable amendments issued from time to time. ("**Master Direction**").

This Policy document envisages the establishment and adoption of measures and procedures relating to KYC, AML and Combating Financing for Terrorism **(CFT)** for GetGrowth in accordance with the requirements prescribed by RBI and as amended from time to time.

2. DEFINITIONS

Unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

"Aadhaar 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', means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information after verifying the information in such manner as may be specified in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

"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", as defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted 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.

"Beneficial Owner (BO)"

a. Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.
   Explanation: For the purpose of this sub-clause-
   i. **"Controlling ownership interest"** means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the Company.
   ii. **"Control"** shall include the right to appoint the majority of the directors or to

control the management or policy decisions including by their shareholding or management rights for shareholder's agreements or voting agreements.

b. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.
c. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
   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.
d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Board" means Board of Directors of the Company.

"Central Identities Data Repository" (CIDR), as defined in Section 2(h) of the Aadhaar Act, means a centralised 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.

"Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) (aa) of the Prevention of Money Laundering Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

"Certified Copy" means comparative copy of the possession of Aadhaar number where offline verification cannot be carried out or officially valid document produced by the customer with the original and recording the same on the copy by the authorized officer of the company.

"Certified Copy of OVD" - Obtaining a certified copy by regulated entity shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the regulated entity.
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 of OVD, 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.

"Company" means GetGrowth Capital Private Limited.

"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.

"Designated Director" means Managing Director or a whole-time Director, duly authorized by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act and the Rules.
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.

"Directors" means an individual Director or Directors on the Board of the Company.

"Digital KYC" means capturing a live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the company as detailed under **Annexure D**.

"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.

"Enrolment number" means "Enrolment ID" as defined in Section 2(1)(j) of the Aadhaar (Enrolment and Update) Regulation, 2016 which means a 28-digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.

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

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

"Non-profit organizations" (NPO) means any entity or organization 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 25 of the Companies Act, 1956 or applicable Section 8 of Companies Act, 2013.

"Officially valid document" (OVD) means the following:

- Passport,
- Driving license,
- Proof of possession of Aadhaar Number
- 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,
- Letter issued by the National Population Register containing details of name and address,
- Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. While opening accounts based on Aadhaar also, the Customer must provide proof of the current address as per extant instructions.

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 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", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, 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.

"Person" has the same meaning assigned in the Act and includes:
a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e),
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

"Principal Officer" means an officer nominated by GetGrowth, responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

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

Explanation: Transaction involving financing of the activities relating to terrorism includes transactions 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)" means an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of the Master Direction.

Terms bearing meaning assigned above, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. **"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.

ii. **"Customer"** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iii. **"Walk-in Customer"** means a person who does not have an account-based relationship with the Company but undertakes transactions with the Company.

iv. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.

v. **"Customer identification"** means undertaking the process of CDD.

vi. **"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.

vii. **"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.

viii. **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC

data to the CKYCR, for individuals and legal entities.

ix. **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

x. **"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.

xi. **"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.

xii. **"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.

xiii. **"Simplified procedure"** means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by the Company and who do not possess any of the six officially valid documents, with the alternate documents prescribed under the two provisos of Section 3(a)(vi) of this Directions.

xiv. **"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.

xv. **"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.

xvi. **"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.

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 Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and 'Aadhaar and other Laws (amendment) Ordinance, 2019', any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

3. OBJECTIVE

The objective of this Policy is to prevent GetGrowth from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Proper KYC verification procedures and Customer Due Diligence (CDD) shall also enable the Company to know/ understand its customers and their financial dealings better which in turn help them manage the risks prudently.

GetGrowth has framed this Policy incorporating the following four key elements:

a) Customer Acceptance Policy;
b) Risk Management;
c) Customer Identification Procedures (CIP); and Customer Due Diligence (CDD) and;
d) Monitoring of Transactions and reporting of Suspicious transactions.

4. CUSTOMER ACCEPTANCE POLICY

GetGrowth shall develop a clear Customer Acceptance Policy laying down necessary criteria for acceptance of customers. The Customer Acceptance Policy shall ensure that the guidelines are in place on the following aspects of customer relationship in GetGrowth:

i. No account is opened in anonymous or fictitious/ benami name(s) and PAN shall be mandatory for each account. Unique Customer Code will be allotted to a single PAN.
ii. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
iii. No transaction or account-based relationship is undertaken without following the CDD procedure.
iv. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
v. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
vi. If an existing KYC compliant customer of the Company desires to open another account or avail another facility, there shall be no need for a fresh CDD exercise.
vii. CDD Procedure is followed for all the joint account holders, while opening a joint account.
viii. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
ix. 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.
x. GetGrowth will take care of the documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time.
xi. Where Permanent Account Number (PAN) is obtained from the customer, the same shall be verified from the verification facility of Income Tax Act.
xii. Where an equivalent e-document is obtained from the customer, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
xiii. Requirements/ obligations under International Agreements - Communications from International Agencies as detailed in Annexure A shall be adhered to.
xiv. Necessary checks and balances to be put into place (at the time of onboarding and periodically thereof) so as to ensure that the identity of the customer does not match with any person having known criminal background or is not banned in any other manner. Customer details should be screened against the following lists:
    a. Individuals and entities in various United Nations Security council resolution lists (UNSCRs) such as UN 1267
    b. Individuals or entities listed under section 51A of Unlawful Activities (Prevention) Act, 1967

c. Individuals and entities in watch list issued by Interpol
d. Reputationally Exposed Person (REP)
e. Politically Exposed Person (PEP)
f. Internal fraud / attempted fraud list (post disbursement)
g. Debarred / negative lists or Regulatory watch list (RBI, SEBI, NHB, IRDA, FIU, etc)

xv. Periodic review of risk categorisation of accounts shall be undertaken as per the defined procedures

The Customer Acceptance Policy shall not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

Accounts of Politically Exposed Persons (PEPs):
PEPs are individuals who are or have been entrusted with prominent public functions e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Company 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 as a customer;
c. the decision to open an account for a PEP is taken at a senior level in accordance with the 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.

The additional measures applicable to PEP as required under the KYC Directions shall also be applied for family members and close relatives of PEP including the beneficial owners.

5. RISK MANAGEMENT

The Board of Directors of GetGrowth has ensured that an effective KYC program is in place and has established appropriate procedures and is overseeing its effective implementation. The program covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has been explicitly allocated within GetGrowth to ensure that GetGrowth's policies and procedures are implemented effectively. The Board has devised procedures for creating Risk Profiles of new customers and will apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

For Risk Management, GetGrowth aim is to identify customers who are likely to pose a higher than average risk of money laundering or terrorist financing and thus shall have a risk-based approach which includes the following.

i. Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of GetGrowth.
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. 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.

iii. Risk categorisation for accounts shall be basis:
- Low Risk: For the purpose of risk categorization, individuals/entities whose identities & source of income can easily be identified should be categorized as Low Risk. The examples of low risk customers are Individual Salaried Customers, Professionals, Retired Individuals, Housewives etc.
- Medium Risk: Customers who are likely to pose a higher than average risk to the Company should be categorized as medium risk. Examples of Medium Risk are self-employed customers having income above a certain threshold, etc.
- High Risk: Customers who are likely to pose a higher than medium risk to the organization should be categorized as high risk. Examples of high risk customers are Politically Exposed Persons (PEPs), persons in negative list, customers who are close relatives of PEPs, customers with dubious reputation as per public information available etc.

Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment:

a. The Company 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.
b. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.
c. The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
d. 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.
e. The company 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, the Company shall monitor the implementation of the controls and enhance them if necessary.

ML / TF Risk Assessment procedures

This section provides a detailed procedure for conducting risk assessment with an aim to reduce and mitigate the ML/TF risk exposure.

Risk Assessment

- The Internal Risk Assessment shall be performed to define ML and TF threats and risks to the company as per the parameters defined in this policy.
- Review shall be done of the existing controls for adequacy and effectiveness and define the overall risk exposure for risk identified.
- Review shall also be done to review the residual risk, if any identified in previous Risk Assessment for the risks which are accepted.

Risk Treatment

- A risk treatment plan shall be developed to prioritize and address the risks identified during the risk assessment phase by way of appropriate risk treatment measures in the form of controls.
- The company shall take appropriate decisions on the acceptance or treatment of the risk. Following are the ways to treat the risks identified during Risk Assessment:
    a) Mitigate Risk: To limit the risk by implementing additional controls that minimize or eliminate the adverse impact of a threat's exercising vulnerability
    b) Transfer Risk: To transfer the risk by using other options to compensate for the loss.
    c) Avoid Risk: To avoid the risk by eliminating the risk cause and/or consequence.
    d) Accept Risk: To accept the potential risk and continue operating the system or to implement controls to lower the risk to an acceptable level.
- Residual risk is the risk left over after implementation of a risk treatment option (recommended controls). It is the risk remaining after exercising one of the options of Mitigation, Transfer, Avoid and Accept.

6. CUSTOMER IDENTIFICATION PROCEDURES (CIP) & Customer Due Diligence (CDD)

Set out below is GetGrowth's adopted Customer Identification Procedures (CIP) and the Due Diligence that shall be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when GetGrowth has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. GetGrowth will obtain sufficient information stated below necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of the business relationship. Being satisfied means that GetGrowth must be able to satisfy the competent authorities like RBI that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer.

For customers that are legal persons or entities, GetGrowth will verify the identity of customers in the following manner:

i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
ii. Verify the legal status of the legal person/ entity through charter documents and Tax registration, etc.
iii. Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person through authentic documents.
iv. Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal Person.

An indicative list of the nature and type of documents/information that may be relied upon for Customer Due Diligence (CDD) procedure are provided in **Annexure B**.

7. MONITORING OF TRANSACTIONS

"Suspicious Transaction" means a 'transaction' including attempted transaction, whether or not made in cash, which, to a person acting in good faith -

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Schedule to the Act, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

On-going Due Diligence:
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 transaction. Company shall make endeavours 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.

Company should pay particular attention to the transactions having high risk. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of Company. Higher risk transaction shall be subjected to intense monitoring. Company shall set key indicators for such transaction 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. Company shall carry out the periodic review of High-risk categorization of transactions and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

The extent of monitoring shall be aligned with the risk category of the customer.

Periodic Updation:
The Company shall adopt a risk-based approach for periodic updation of KYC. However, periodic 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 from the date of opening of the account / last KYC updation as detailed in **Annexure C**.

8. 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. The Company shall,

a. maintain all necessary records of transactions between the Company 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. Maintain the records of alerts generated, the analysis of alerts, details of explanations sought and provided, the documentary evidences including the bank/demat statements, etc. for at least five years or for such a higher period as may be prescribed under the applicable laws and regulations from time to time.
d. make available the identification records and transaction data to the competent authorities upon request;
e. 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);

f. 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.

g. 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;

h. 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.

9. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA

The Company 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.

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 Company 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.

10. SECRECY OBLIGATIONS AND SHARING OF INFORMATION:

The Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

Additionally, the Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the company and customer except in the following situations:

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

11. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

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

A register of attendance or participation in such an education/ training program shall be maintained for the employees.

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

Adequate steps to be taken to comply with the reporting requirements under the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS), if and as applicable.

13. Principal Officer and Designated Director

The Company shall designate a "Principal Officer'' who shall be "Senior Management Person" for all KYC/AML matters. The Principal Officer shall be responsible for implementation and compliance of this policy shall include the following:

- Compliance of the provisions of the PMLA Guidelines
- Monitoring the implementation of KYC AML Policy
- Reporting of Transactions and sharing of information as required under the law
- Ensure that the Company discharges its legal obligation to report suspicious transactions to the concerned authorities.

Name, Designation and Contact details including address of the Principal Officer and change therein shall be intimated to the Office of the Director-FIU-IND.
"Designated Director" means a person designated by the Board of Directors to ensure overall compliance with the obligations imposed under PMLA and the Rules framed there under, as amended from time to time, and includes the Managing Director or a Whole-time Director duly authorized by the Board of Directors.

The Company shall appoint a Designated Director and communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND and update the same whenever there is any change.

14. COMPLIANCE OF KYC POLICY

a. The Audit Committee shall be reported in the form of a note on a quarterly basis about the status of KYC compliance of all the borrowers of the Company in accordance with this policy.
b. The internal auditors need to provide a quarterly update to the Audit committee on KYC compliance and the procedures to be followed.
c. The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

Annexure A

The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists as as follows:

1. 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
2. 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

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other 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 (Annex I of the Master Direction) 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 above do not preclude the Company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.*
c. 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.

Annexure B

Individuals/ Beneficial Owner – OVD Requirements:

S. No.	OVD	ID Proof	Address Proof*
1	Valid Passport	Acceptable	Acceptable
2	Driving License	Acceptable	Acceptable
3	Voter ID Card	Acceptable	Acceptable
4	Aadhaar Card#/PAN Card	Acceptable	Acceptable
5	Job Card issued by NREGA	Acceptable	Acceptable
6	Letter issued by the National Population Register	Acceptable	Acceptable

***** Where the OVD furnished by the customer does not have updated address, the following documents 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;

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.

The Company shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means.
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, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.
The Company may carry out offline verification of a customer if he/ she is desirous of undergoing Aadhaar offline verification for identification purpose. In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer.

Non-Individuals – OVD Requirements:

Constitution	KYC Documents
Proprietorship	Any two of the following documents in the name of the proprietary concern needs to be obtained if the loan is in the name of Proprietorship Firm (Main Applicant): 1. Registration certificate 2. Certificate/license issued by the municipal authorities under Shop and Establishment Act. 3. Sales and income tax returns. 4. CST/VAT/ GST certificate (provisional/final) 5. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. 6. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of

	the proprietary concern by any professional body incorporated under a statute 7. 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 8. Utility bills such as electricity, water, landline telephone bills (should not be more than two months old Other than the above mentioned, PAN of the Proprietor needs to be obtained. In cases where it is not possible to furnish two such documents, only one of those documents as proof of business/activity, may be accepted. Provided contact point verification and collecting such other information and clarification as would be required to establish the existence of such firm is undertaken and is satisfied that the business activity has been verified from the address of the proprietary concern.
Partnership Firm	The certified copies of each of the following documents shall be obtained: 1. Registration certificate 2. Partnership deed 3. Permanent Account Number of the partnership firm 4. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Companies (Pvt Ltd /Ltd /OPC)	The certified copies of each of the following documents shall be obtained: 1. Certificate of incorporation 2. Memorandum and Articles of Association 3. Permanent Account Number of the company 4. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf 5. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
Trust	The certified copies of each of the following documents shall be obtained: 1. Registration certificate 2. Trust deed 3. Permanent Account Number or Form No.60 of the trust 4. Documents of the person holding an attorney to transact on its behalf
Unincorporated association or a body of individuals	The certified copies of each of the following documents shall be obtained: 1. Resolution of the managing body of such association or body of individuals 2. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals 3. Power of attorney granted to transact on its behalf 4. Documents of the person holding an attorney to transact on its behalf 5. Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals

	Explanation: - Unregistered trusts/ partnership firms shall be included under the term 'unincorporated association'. - Term 'body of individuals' includes societies.
Juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats	The certified copies of each of the following documents shall be obtained: 1. Document showing name of the person authorised to act on behalf of the entity 2. Documents of the person holding an attorney to transact on its behalf 3. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Common Mandatory Documents:

1. Recent photograph of Applicant, Co- Applicant, Beneficial Owners or Authorized Persons holding an attorney to transact on behalf of the Applicant. However, digitally captured photographs are acceptable.
2. GST Registration Certificate of the Entity
3. Certified copy of officially valid documents (OVD) as proof of identity and address of Authorized Persons and Co-Applicant

Identification of Beneficial Owner:

For a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 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.

OVD Verification Process:

The KYC documents/ Officially Valid Documents (OVD) can be verified by the employees/ representatives of GetGrowth and/or third party.

However, in case of a third party, the Company may, rely on customer due diligence done by such third party, subject to the following conditions:

a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
b) 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 PML Act.
d) The third party shall not be based in a country or jurisdiction assessed as high risk.
e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

CDD Procedure and sharing KYC Information with Central KYC Records Registry (CKYCR):

a. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security 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.
b. In terms of provision of Rule 9(1A) of PML Rules, the Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
c. The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
d. The Company shall upload KYC records pertaining to accounts of LEs opened, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.
e. Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual/LE as the case may be.
f. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
g. Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
    i. there is a change in the information of the customer as existing in the records of CKYCR;
    ii. the current address of the customer is required to be verified;
    iii. the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

V-CIP:

V-CIP can be undertaken to carry out:

i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
ii. Provided that in case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned above, apart from undertaking CDD of the proprietor.
iii. Updation/Periodic updation of KYC for eligible customers.

V-CIP Procedure:

i. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
ii. If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.
iii. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
iv. Any prompting, observed at end of customer shall lead to rejection of the account opening process.

v. The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
   - OTP based Aadhaar e-KYC authentication
   - Offline Verification of Aadhaar for identification
   - KYC records downloaded from CKYCR using the KYC identifier provided by the customer
   - Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

   The Company shall ensure to redact or blackout the Aadhaar number.
   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.
   Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.

vi. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

vii. The Company 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 including through Digilocker.

viii. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

ix. The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

x. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

Annexure C

A. Individual Customers:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of the Company), letter etc.

ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, the Company, at its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

B. Customers other than individuals:

i. **No change in KYC information:** In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. **Change in KYC information:** In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

C. Additional measures: In addition to the above, the Company shall ensure that,

i. The KYC documents of the customer as per the current CDD standards are available with it. This is applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

ii. Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained

from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, the Company may consider making available the facility of periodic updation of KYC at any branch.

v. The Company shall adopt a risk-based approach with respect to periodic updation of KYC.

vi. The Company shall ensure that the KYC policy and processes on updation/ periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

Annexure D

Digital KYC Process

A. The Company 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 Company.

B. The access of the Application shall be controlled by the Company and it shall 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 the Company to its authorized officials.

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

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

E. The Application 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 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/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

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

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 Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

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 Company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the Company 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 Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.