'KNOW YOUR CUSTOMER' (KYC) POLICY AS PER ANTI MONEY LAUNDERING STANDARDS

IIFL WEALTH PRIME LIMITED (hereinafter referred to as **"IIFLW Prime" / "the Company"**), in compliance with the Reserve Bank of India (RBI) Master Direction – Know Your Customer (KYC) Direction, 2016 no. DBR.AML.BC.NO.81/14.01.001/2015-16 dated February 25, 2016 (updated as on May 29, 2019) in lieu of the partially repealed circulars of RBI DBOD.BP.BC.57/21.01.001/95-Paragraph2(b) dated Ma 4, 1995 and DBS.FGV.BC.56.23.04.001/98-99 paragraph "(b) concept of "know Your Customer" (para. 9.2)" with any amendments/ re-enactments thereof issued from time to time ("**RBI KYC Directions**") and the Prevention of Money Laundering Act, 2002 read with the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 with any further amendments/ re-enactments thereof issued from time to time ("**PMLA**") and thereafter and is subject to the final judgement of the Hon. Supreme Court in the case of Justice K. S. Puttaswamy (Retd.) & Anr. V. Union of India, W.P. (Civil), is adopting the Know Your Customer Policy (KYC) Policy with the following amended guidelines on KYC process and documentation:

1. The Company shall follow customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. The policy is based on Anti Money Laundering (AML) standards. Information collected from the customer for the purpose of opening of account shall be kept confidential and the Company shall not divulge any details thereof for cross selling or any other purposes. Information sought from the customer shall be relevant to the perceived risk, shall not be intrusive, and shall be in conformity with the guidelines issued by RBI from time to time. Any other information from the customer shall be sought separately with his/ her/ its consent and after opening the account.
2. The objective of the KYC policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/ understand its customers and their financial dealings better, which in turn help the Company to manage its risks prudently. The Company has framed its KYC policy incorporating the following four key elements:
   (i) Customer Acceptance Policy;
   (ii) Customer Identification Procedures;
   (iii) Monitoring of Transactions/ On-going Due Diligence; and
   (iv) Risk Management.
3. For the purpose of the KYC policy:
   a) "**Aadhaar number**", shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
   b) "**Authentication**", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. i.e. process by which the Aadhaar Number along with demographic information or biometric information of an individual is submitted to the central Identities Data Repository for its verification and such repository verifies the correctness, or the lack thereof, on the basis of information available with it.
   c) "**Beneficial Owner**" refers to the natural person(s) who ultimately owns or controls a customer and/ or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

d) "**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 (authentication) regulations.

e) **"Certified Copy"** - Obtaining a certified copy by the Regulated Entity shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Regulated Entity.

f) 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.

g) "**Customer**" means a person that engages in a financial transaction or activity with the Company/ NBFCs and includes a person on whose behalf the person that engages in the transaction or activity is acting.

h) "**Customer Due Diligence (CDD)**" means identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'proof of identity' and 'proof of address'.

i) "**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.

j) "**Digital KYC**" - as capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Reporting Entity (RE) as per the provisions contained in the Act. Steps to carry out the Digital KYC process have also been stipulated in Annexure III

k) **"Digital Signature**" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

l) "**Designated Director**" means a person designated by the NBFC to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall include Managing Director or a whole-time director, duly authorised by the Board of Directors of the Company.

m) **"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

n) "**E-KYC authentication facility**", as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through

a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction.

o) -"**Identity information**", as defined in sub-section (n) of section 2 of the Aadhaar Act, in respect of an individual, includes individual's Aadhaar number, biometric information and demographic information.

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

q) **"Office of Foreign Assets Control (OFAC)"** of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.

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

s) **"United Nations Security Council (UNSC)**" establishes sanctions committee which publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name, and the consolidated sanctions list includes all individuals and entities subject to sanctions measures imposed by the UNSC.

t) "**Officially Valid Document**" (OVD) means the passport, the driving licence, Proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name and 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.*

u) **-Politically Exposed Persons (PEPs)**" are:

(i) individuals who are or have been entrusted with prominent public functions domestically or by a foreign country, e.g., Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials;

(ii) international organization PEPs who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors and members of the board or equivalent functions, and

(iii) family members related to PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership; and

(iv) close associates are individuals who are closely connected to a PEP, either socially or professionally.

v) "**Principal Officer**" means an officer designated by the Company.

w) "**Video based Customer Identification Process (V-CIP)**": a method of customer identification by an official of the RE 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.

4. Customer Acceptance Policy (CAP):

The criteria for acceptance of customers are as follows:

(i) No account shall be opened in anonymous or fictitious/ benami name(s);

(ii) No transaction or account-based relationship will be undertaken without following the Customer Due Diligence (CDD) procedure.

a. The information to be sought for KYC purpose while opening an account and during the periodic updates as specified, should be obtained.

b. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.

c. CDD procedure is followed for all the joint account holders while opening a Joint Account.

(iii) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity;

(iv) Parameters of risk assessment in terms of the customers' identity, social/ financial status, nature of business activity, information about the clients' business and their locations, etc. have been defined to enable categorization of customers into low, medium and high risk. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities or other entities may also be factored in 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 RBI KYC Directions and PMLA as issued from time to time;

(v) The Company shall not open an account where it is unable to apply appropriate CDD measures, i.e., the Company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. 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;

(vi) Before opening a new account necessary screening will be performed so as to ensure 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 or whose name appears in the lists circulated by RBI/ SEBI/ NHB/ IRDA, United Nations Security Council (UNSC), OFAC, as per section 51A of the Unlawful Activities (Prevention) Act, 1967, watch list by Interpol, etc. These are done using the list/ information/ databases available on World-check, Watch-out Investors, website of OFAC, UNSCR (as mentioned below) or such other information sources/tools.

Web-link(s) for client regulatory verification on OFAC and UNSCR list are as under:

OFAC Link: https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

UNSCR Link: The details of the two lists are as under:

(a) The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl
https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

(b) **The "1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl

The Company shall prepare a profile for each new customer based on risk categorization, as provided subsequently in this policy.

(vii) For the purpose of risk categorization, individuals (other than High Net Worth individuals) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

Customers that are likely to pose a higher than average risk to the company shall be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and client profile etc. The Company shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring enhanced due diligence shall include (a) high net worth individuals, (b) trusts, charities, NGOs and organizations receiving donations, (c) companies having close family shareholding or beneficial ownership, (d) firms with 'sleeping partners', (e) Politically Exposed Persons, (f) non-face to face customers, and (g) those with dubious reputation as per public information available, etc.

In case of non-face-to-face customer, Company shall ensure that the first payment is to be effected through the customer's KYC-complied account with another registered entity for enhanced due diligence.

While criteria for defining high net worth is not defined in the existing RBI Circulars applicable to NBFCs, this is being internally defined as net worth of more than INR 100 Crore.

The adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

5. Customer Identification Procedure (CIP):

5.1 Customer Identification Procedure to be carried out at different stages as under:

- Commencement of an account-based relationship with the customer;
- When the Company has a doubt about the authenticity or adequacy of the customer identification data obtained by the Company. Customer identification means identifying the customer and verifying his/ her/ its identity by using reliable, independent source documents, data or information; and
- Carrying out a financial transaction.

5.2 The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company should be able to satisfy the competent authorities 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 (individual, corporate, etc.). The Company shall ensure that decision-making functions of determining compliance with KYC norms shall not be outsourced.

5.3 For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company, shall at their 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 days from the third party or from the Central KYC Records Registry.

ii) Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements shall be made available from the third party upon request without delay.

iii) The third party is regulated, supervised or monitoring for, and has measures in place for, compliance with CDD and record-keeping requirements in line with the requirements and obligations under the PML Act.

iv) The third party shall not be based in a country or jurisdiction assessed as high risk.

v) The ultimate responsibility for CDD and undertaking enhanced due diligence measures, as applicable, will be with the Company.

5.4 The Company shall allot Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships. The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise.

5.5 Procedure for obtaining Identification Information -

5.5.1 For undertaking CDD, the Company shall obtain the following information from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity: From an individual who is eligible to be enrolled for an Aadhaar number, the Company shall obtain (a) from an individual who is eligible for enrolment of Aadhaar, the Aadhaar; the Permanent Account Number (PAN) or Form No. 60 as defined in the Income-tax Rules, 1962, as amended from time to time,;

Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case the PAN is not submitted, one certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained.

Provided further, that from an individual, who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and who does not submit Aadhaar or proof of application of enrolment for Aadhaar, the following shall be obtained:

a) Certified copy of an OVD containing details of identity and address; and

b) One recent photograph.

5.5.2 From an individual who is not eligible to be enrolled for an Aadhaar number, or who is not a resident, the following shall be obtained:

a) PAN or Form No. 60 as defined in Income Tax Rules, 1962, as amended from time to time.
b) One recent photograph; and
c) A certified true copy of an OVD containing details of identity and address.

Provided that in case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the government departments of foreign jurisdiction and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided further that while opening accounts of legal entities, in case, PAN of the authorised signatory or the power of attorney holder is not submitted the certified copy of OVD of the authorised signatory or the power of attorney holder shall be obtained, even if such OVD does not contain address.

Provided that where PAN is obtained, the same shall be verified from the verification facility of the issuing authority. Also where an equivalent e-documents is obtained from the customer, Company shall verify the digital signature as per the provision of the Information technology Act, 2000.

Explanation: Aadhaar number shall not be sought from individuals who are non 'residents' as defined under the RBI Directions. A declaration to the effect of individual not being eligible for enrolment of Aadhaar may be obtained by the Company. Customers, at their option, shall submit one of the five OVDs.

5.5.3 In case the identity information relating to the Aadhaar number or PAN submitted by the customer does not have current address, an OVD as defined above shall be obtained from the customer for this purpose.

Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:

a) Utility bill which is not more than two months old of any service provider (electricity, telephone post paid mobile phone, piped gas, water bill);
b) Property or municipal tax receipt;
c) Pension or family pension payment orders (PPOs issued to retired employees by government departments or Public Sector Undertakings, if they contain the address;
d) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory borides, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

Provided further that the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

5.5.4 The Company, at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/ No authentication. Provided,

a) Yes/ No authentication shall not be carried out while establishing an account-based relationship.

b) In case of existing accounts where Yes/ No authentication is carried out, the Company shall ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/ no authentication.

c) Yes/ No authentication in respect of beneficial owners of a legal entity shall suffice in respect of existing accounts or while establishing an account-based relationship.

d) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Company. Further, while uploading KYC information to CKYCR, Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

e) Company shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act. Or proof of possession of Aadhaar no. where offline verification can be carried out or proof of possession of Aadhaar no. where offline verification cannot be carried out or any OVD or equivalent e-documents thereof containing the details of his identity and address.

f) Company may undertake live V-CIP , to be carried out by the officials for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere the process (Refer annexure IV).

5.5.5 In case the customer eligible to be enrolled for Aadhaar and obtain a PAN, referred to in section 5.5.1 above, the customer shall submit the Aadhaar number to the Company till a date to be notified subsequent to the pronouncement of final judgement by Supreme Court in W.P. (C) 494/2012.

5.5.6 The customer, eligible to be enrolled for Aadhaar and obtain the PAN, except one who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya already having an account-based relationship with the Company, shall submit the Aadhaar number and PAN/ form 60 till a date to be notified subsequent to pronouncement of final judgement by Supreme Court in W.P. (C) 494/2012.

5.6 Simplified procedure for opening accounts by the Company - In case a person who desires to open an account is not able to produce any of the OVDs, Company may open accounts subject to the following condition:

(a) Obtain a self-attested photograph from the customer.

(b) The designated officer of the Company certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) The account shall remain operational initially for a period of twelve months, within which CDD as mentioned under clause 5.5 above.

(d) balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.

(e) the total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (e) and (f) above are breached by the him.

(g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the

total balance in all the accounts taken together exceeds the limits prescribed in direction (4) and (e) above.

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

5.7 Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution, are given in **Annexure - I**. If the Company accepts such accounts in terms of the Customer Acceptance Policy, the Company shall take reasonable measures to identify the beneficial owner(s) and verify his/ her/ their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

5.8 An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the KYC Documentation Policy annexed as **Annexure-II**.

6. <u>Monitoring of Transactions/ On-going Due Diligence:</u>

a) The Company shall pay special attention to all large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

b) The Company shall prescribe threshold limits for specific categories of accounts and pay particular attention to the transactions which exceed prescribed thresholds, based on income and / or net worth of the customer.

c) Currently, no cash transactions are done by the Company, since all disbursements and repayments are made through normal banking channels only. However, should it ever be necessary to operate cash, transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

d) High-risk accounts shall be subjected to intensify monitoring and enhanced due diligence. The Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. The Company shall put in place a system of periodical review of risk categorization of accounts, with such periodicity being at least once in 6 (six) months and the need for applying enhanced due diligence measures.

e) The records of transactions in the accounts shall be preserved and maintained as required in terms of section 12 of the PML Act, 2002. The Company shall report the transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, to the appropriate law enforcement authority.

f) While currently, no cash transactions are undertaken, in the unforeseen event of such transactions taking place, the Company will maintain a proper record of all cash transactions (deposits and withdrawals) of Rs.10 lakh and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

7. <u>Risk Management:</u>

a) Through this policy, the Board of Directors of the Company is ensuring the formal documentation of its KYC programme. The management will establish appropriate procedures to ensure its effective implementation.

b) The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance

function would provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The audit machinery shall be staffed adequately with individuals who are well-versed in such policies and procedures. The Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals.

c) The Company shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC and AML procedures. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policy and implement the same consistently.

d) The Company will carry out Money Laundering (ML) and Terrorist Financing (TF) risk assessment exercise on Yearly basis and will identify money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

e) The Company shall constitute an Anti-Money Laundering Committee ("AML Committee") comprising of (i) CEO and Whole Time Director, (ii) Chief Operations Officer, (iii) Operations Representative, (iv) Chief Risk Officer and (v) Compliance Officer of the Company and the Terms of Reference of the said AML Committee shall be as mentioned below:

   i. To define, approve, modify the AML Policy and procedures & Control / monitoring mechanism
   ii. To provide framework for clients acceptance criteria
   iii. To define sub-delegation of authority matrix
   iv. To define KYC and additional KYC requirement for clients
   v. To define Reporting structure for Suspicious Transactions
   vi. To design programs to educate the staff on AML.
   vii. To appoint auditor for AML purpose and define the scope of audit
   viii. To review audit report provide the risk mitigation measures.
   ix. To place the audit report along with comments of committee, at the Board Meeting.

8. <u>Introduction of New Technologies:</u>

The Company shall pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent its use in money laundering schemes.

9. <u>Periodic Updation/ Review of KYC for the Existing Accounts:</u>

a) The Company shall also apply this policy to the existing customers on the basis of materiality and risk. Moreover, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account shall trigger a review of the CDD measures.

b) The Company shall consider applying monetary limits to such accounts based on the nature and type of the account. All the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'.

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

d) The Company shall carry out periodic updations at least once in every 2 years for high risk customers, once in every 8 years for medium risk customers and once in every 10 years for low risk customers, subject to the following conditions:

(1) The Company shall carry out;

- PAN verification from the verification facility available with the issuing authority; and
- Authentication, of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.
- In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
- 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.
- In case of legal entities, the Company shall review the documents sought at the time of opening of account and obtain fresh certified copies.

(2) The Company 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 customer is required to establish the bona-fides. Normally, OVD/ Consent forwarded by the customer through mail/ post, etc. shall be acceptable.

(3) The Company shall ensure to provide acknowledgment with date of having performed KYC updation.

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

10. <u>Applicability to branches and subsidiaries outside India:</u>

The policy shall also apply to the branches (if any) and majority owned subsidiaries located abroad (if any), especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same would be brought to the notice of the RBI.

11. <u>Appointment of Principal Officer:</u>

The Company has appointed a senior management officer designated as the Principal Officer. The Principal Officer shall be located at the head office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, the Company and any other institution, which are involved in the fight against money laundering and combating financing of terrorism.

12. <u>Record Management:</u>

In order to maintain, preserve and report the customer account information, with reference to provisions of PML Act and Rules, the Company shall:

1) maintain all necessary records of transactions between the Company and the customer for at least 5 (five) years from the date of transaction;
2) 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 5 (five) years after the business relationship is ended;
3) make available the identification records and transaction data to the competent authorities upon request;

4) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005;
5) maintain all necessary information in respect of transactions prescribed under PML Rule 3 as to permit reconstruction of individual transaction, including the nature, amount and date of transaction and the parties to the transaction;
6) evolve a system for proper maintenance and preservation of account information in a manner that allows easy and quick retrieval of data whenever required or requested by the competent authorities; and
7) maintain records of identity and address of the customers and records in respect of transactions referred to in PML Rule 3 in hard or soft format.

The Company shall upload the KYC data pertaining to all new individual accounts opened on or after April 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

Where the customer already has a Central KYC (CKYC) 14-digit acknowledgement number, his / her documents need not be obtained again. Documents relating to identification and address can simply be downloaded from the CKYC website https://testbed.ckycindia.in/ckyc/index.html. However, loan agreements and finance related documents will still need to be signed/ provided by the customer. Details / documents collected by the Company also need to be uploaded into the CKYC website within 3 (three) days of the commencement of the relationship.

ANNEXURE – I

Customer Identification Requirements – Indicative Guidelines

A) Trust/Nominee or Fiduciary Accounts:

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The Company should determine whether the customer is acting on behalf of another person as trustee/ nominee or any other intermediary. If so, the Company 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. While opening an account for a trust, the Company 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', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined. 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.

B) Accounts of companies and firms:

The Company shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Company. The Company shall examine the ultimate beneficial ownership and 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 shall be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

C) Client accounts opened by professional intermediaries:

1) When the Company has knowledge or reason to believe that the customer account opened by a professional intermediary is on behalf of a single customer, that the customer must be identified.
2) The Company may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. However, the Company shall not open accounts of such professional intermediaries, viz., lawyers/chartered accountants or stockbrokers, who are bound by any customer confidentiality that prohibits disclosure of the customer details to the Company.
3) Where funds held by the intermediaries are not co-mingled at the Company and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled, the Company shall still look through to the beneficial owners.
4) Where the Company rely on the CDD done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements for the customers.

D) Accounts of Politically Exposed Persons (PEPs) (includes a PEP is the beneficial owner):

1) The Company should gather sufficient information including information about the sources of funds accounts of family members and close relatives, on any person/customer of this

category intending to establish a relationship and check all the information available on the person in the public domain.

2) The Company shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.
3) The decision to open an account for PEP should be taken at a senior level in accordance with the Customer Acceptance Policy of the Company.
4) The Company shall also subject such accounts to enhanced monitoring/ due diligence on an ongoing basis.
5) The Company shall obtain the approval of senior management in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, to continue the business relationship.
6) The Company shall ensure the applicability of CDD measures to PEPs including enhanced monitoring on an on-going basis.

ANNEXURE - II

KNOW YOUR CUSTOMER (KYC) DOCUMENTATION POLICY

PURPOSE:

The purpose of this document is to establish Know Your Customer (KYC) documentation policy for IIFL Wealth Prime Limited ("**IIFLW Prime**"). All the loans originated by IIFLW Prime would follow this KYC documentation policy.

BACKGROUND:

This KYC documentation policy will enable us to make changes in only one document which will be followed by all products/businesses and will standardize the KYC documentation policy throughout the organization.

Documentation requirements have been laid down for each client type. The basic documents are the minimum required by law for AML and KYC for identification and address. Additional documents are those that provide details of a customer's sources of income, beneficial ownership (in the case of entities) and bank account(s) for transacting with the Company:

INDIVIDUAL:

S/N.	KYC Document to be obtained as mentioned in clause 5.5 above	Id Proof	Address Proof
1.	PAN Card	Acceptable	Not Acceptable
2.	Driving license	Acceptable	Acceptable
3.	Valid Passport	Acceptable	Acceptable
4.	Voter's ID Card	Acceptable	Acceptable
5.	Job card issued by NREGA duly signed by an officer of the State Government	Acceptable (If carries Photograph)	Acceptable (If carries Photo & Address)
6.	The letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number	Acceptable	Acceptable
7.	OVDs in the circumstance specified in clause 5.5.3 above	Not Acceptable	Acceptable
8.	Bank Statement not older than last two months	Not Acceptable	Acceptable

Additional Documents (Individual):

S/N.	Document Name	Remarks
1.	RTGS Letter/Disbursement request	Format available in LAS booklet
2.	Original Cancelled cheque	Of the bank account where the loan is to be disbursed
3.	Last 2 FY Income Tax Return (ITR) copies alongwith Computation of Income or Latest Net Worth Certificate issued by a Chartered Accountant or Latest Audited Balance Sheet.	
4.	CA attested Balance Sheet and P&L for the last 2 FYs ***OR*** CA attested Net Worth Certificate (not more than 1 year old) **where last FY ITR is showing as a loss or where ITR is not available**	
5.	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.

NON-INDIVIDUALS:

Proprietorship -

Category	KYC Document
Proprietorship	A) Identification information as mentioned under clause 5.5 above in respect of the individual (proprietor) (as per 'Individual table' given above). These need to be attested by the Proprietor with the stamp of the business entity. B) ^Any two of the following documents in the name of the proprietary concern need to be obtained as proof of business/activity: 1. Registration Certificate. 2. Certificate/license issued by the Municipal authorities under Shop & 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 DGFT / License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. 7. Utility bills such as electricity, water, and landline telephone bills (not older than last two months) in the name of the proprietary concerns. 8. Complete Income Tax Return (not just the acknowledgment) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities. ***^Note:*** *In cases where the Company are satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/ activity provided the Company undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.*
Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.

Additional Documents (Sole Proprietorship):

S/N.	Document Name	Remarks
1.	Cancelled cheque of the Firm	Of the bank account where the loan is to be disbursed
2.	Last 2 FY Income Tax Return (ITR) copies alongwith Computation of Income or Latest Net Worth Certificate issued by a Chartered Accountant or Latest Audited Balance Sheet	
3.	CA attested Balance Sheet and P&L for the last 2 FYs OR CA attested Net Worth Certificate (not more than 1 year old) **where last FY ITR is showing as a loss or where ITR is not available.**	
4.	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.

Hindu Undivided Family (HUF) -

Category	KYC Document
HUF	• Pan card copy of HUF attested by Karta (more specifically in the manner specified in clause 5.5 above). • Latest Address proof of HUF attested by Karta like Bank Statement (not older than last two months) (more specifically in the manner specified in clause 5.5 above). • Identification information as mentioned under clause 5.5 above in respect of the Karta (individual) (as per 'Individual table' given above).

Additional Documents (HUF):

S/N.	Document Name	Remarks
1.	RTGS Letter/Disbursement request	Format available in LAS booklet
2.	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.
3.	Copy of cancelled cheque	Of the bank account where the loan is to be disbursed
4.	Last 2 FYs ITR copies of HUF alongwith Computation of Income or Latest Net Worth Certificate issued by a Chartered Accountant or Latest Audited Balance Sheet	
5.	CA attested Balance Sheet and P&L for the last 2 FYs OR CA	

	attested Net Worth Certificate (not more than 1 year old) **where last FY ITR is showing as a loss or where ITR is not available**	

Companies/ Corporates -

Category	KYC Document
Companies/ Corporates	Certified copy of: • Certificate of incorporation; • Memorandum and Articles of Association; • Permanent Account Number of the Company; • A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf on company letter head as per format circulated separately. To be signed (with stamp) by Managing Director or Chairman or full time Company Secretary or at least two Directors (who are not the persons getting authorised); • Identification information as mentioned under clause 5.5 above in respect of the person holding power of attorney to transact on its behalf. • Documents relating to beneficial owner, the managers, officers or employee as the case may be, holding an attorney to transact on the Company's behalf.

Additional documents (Companies/ Corporate):

Sr. No.	Document Name	Remarks
1.	RTGS Letter/Disbursement request	Format available in LAS booklet
2.	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.
3.	Pan card copy/Latest Address of Company, Authorised Signatories/Directors	To be signed by respective authority
4.	List of Authorized Signatories, List of Directors and Shareholding Pattern (with percentage) as on date	On company letter head.
5.	MOA/AOA & Certificate of Incorporation, MCA site print of Company and Signatory list	-
6.	Cancelled cheque leaf	Of the bank account where the loan is to be disbursed
7.	Last 2 FYs ITR copies alongwith Audit Report	Mandatory

8.	CA attested Balance Sheet and P&L for the last 2 FYs OR CA attested Net Worth Certificate (not more than one year old) - **where ITR is not available or last FY ITR is showing a loss**	
9.	UBO declaration form	Format available in LAS booklet. Should be complete filled up. KYC documents and ITR for past two years required for UBO.

Partnership Firm -

Category	KYC Document
Partnership Firms	Certified copy of: • Registration certificate; • Partnership deed; • List of all partners and their Profit / Loss sharing ratios on the firm's letterhead, signed by authorized signatory • An OVD (Authority Letter, on the firm's letterhead, signed by all partners) in respect of the authorized signatories / person(s) holding an attorney to transact or execute documents on behalf of the firm. • Identification information as mentioned under clause 5.5 above in respect of the person holding power of attorney to transact on its behalf. • Documents relating to beneficial owner, the managers, officers or employee as the case may be, holding an attorney to transact on the Company's behalf.

Additional Documents (Partnership Firms):

Sr. No.	Document Name	Remarks
1	RTGS Letter/Disbursement request	Format available in LAS booklet
2	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet.
3	Last 2 FYs ITR copies alongwith Computation of Income or Latest Networth Certificate issued by a Chartered Accountant or Latest Audited Balance Sheet	
4	CA attested Balance Sheet and P&L for the last 2 FYs OR CA attested Net worth Certificate (not more than one year old) - **where ITR is not available or last FY ITR is showing a loss**	

5	Cancelled cheque leaf	Of the bank account where the loan is to be disbursed
6	UBO declaration form	Format available in LAS booklet. Duly filled up. KYC documents and ITR for past two years required for UBO.

Trust /Association of Persons (AOP) -

Category	KYC Document
Trust/ Association of Persons (AOP)	Certified copy of: • Registration certificate; • Trust deed; and • Board of Trustees ***OR*** Managing Committee resolution duly signed (with stamp) by Managing Trustee ***OR*** Chairman Or full time Company Secretary or at least two Trustees (other than those being authorised). • List of beneficial owners / beneficiaries, Author of the trust and Trustees on the letter head. • Identification information as mentioned under clause 5.5 above in respect of the person holding power of attorney to transact on its behalf. • Documents relating to beneficial owner, the managers, officers or employee as the case may be, holding an attorney to transact on the Company's behalf.

Additional Documents (Trust /Association of Persons (AOP):

Sr. No.	Checklist of documents	Remarks
1	RTGS Letter/Disbursement request	Format available in LAS booklet
2	Requirements relating to Deed of Guarantee **- on a case to case basis, where Guarantee is accepted**	KYC documents of Guarantor along with last 2 FYs ITR copies alongwith latest net-worth certificate copy duly certified by Chartered Accountant or Latest Audited Balance Sheet
3	Board / Trustee Resolution authorising borrowing, and persons authorised to transact	On Letter head as per format. To be signed (with stamp) by Managing Trustee Or Chairman Or full time Company Secretary or at least two Non-Authorised Trustees of the BR.
4	Last 2 FYs ITR copies alongwith Computation of Income or Latest Networth Certificate issued by a Chartered Accountant or Latest Audited Balance Sheet	
5	CA attested Balance Sheet and P&L for the last 2 FYs OR CA attested Net worth Certificate (not more than one year old) - **where ITR is not available or last FY ITR is showing a loss**	
6	Copy of cancelled cheque	Of the bank account where the loan is to be disbursed

7	UBO declaration form	Format available in LAS booklet. Duly filled up. KYC documents and ITR for past two years required for UBO.

Un-incorporated Association or a Body of Individuals -

Category	KYC Document
Unincorporated Association or Body of Individual (includes societies)	Certified copy of: • Resolution of managing body of such association or body of individuals; • Power of Attorney granted to transact on its behalf. • Such information as the company requires to collectively establish the legal existence of such an association or body of individual. • Identification information as mentioned under clause 5.5 above in respect of the person holding power of attorney to transact on its behalf. • Documents relating to beneficial owner, the managers, officers or employee as the case may be, holding an attorney to transact on the Company's behalf. *Explanation: Unregistered trusts/ partnership firms shall be included under the term "unincorporated association".* *Explanation: Term 'body of individuals' includes societies.*

Juridical Persons -

Category	KYC Document
Juridical persons (Government or its Departments, societies, universities and local bodies like village panchayats)	Certified copy of: • Document showing name of person authorised to act on behalf of the entity; • Aadhaar/ PAN/ OVDs for proof of identity and address in respect of the person holding a power of attorney to transact in its behalf; and • Such documents as may be required by the company to establish the legal existence of such an entity. • Documents relating to beneficial owner, the managers, officers or employee as the case may be, holding an attorney to transact on the Company's behalf.

Documentation for addition for 3rd party pledgor/guarantor:

1. 3rd party pledgor agreement.
2. 3rd party pledgor PoA.
3. All KYC documents of the 3rd party pledgor.
4. All KYC documents of the Guarantor as prescribed above

NOTE:

Documents and details required under section 285BA of the Income Tax Act, for the purpose of compliance with reporting obligations under Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standards (CRS) also may need to be obtained from customers. These are contained

in Rules 114F-114H of the Income Tax Rules. This would be required where the customer has a relationship beyond just taking loans with IIFLW Prime and intends to use us as a depositary institution or an investment entity as defined in the Income Tax Rules.

EXHIBIT – 1

1. Commissioned officers of the Indian Armed Forces.
2. Officers from the All-India Civil Services (IAS, IPS, IFS, etc.).
3. Engineering Services officers.
4. State Civil Service officers (executive) in the State Governments (PCS/SCS/PPS/upper subordinate officers).
5. Senior Physician (C.M.O.) in State/Central Hospital.
6. Senior Surgeons of Government health service.
7. Chief Pharmacist and beyond All Officers in Pharmacy Cadres State/Central Hospital.
8. Chief Engineers of Central Public Works Department.
9. Magistrates and above in the judicial services.

Annexure III

Digital KYC process

A. The RE 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 REs.

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

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

D. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

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

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. 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 RE, 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 RE 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 RE 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.

Annexure IV
Process for V-CIP

i. The official of the company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and shall obtain the identification information through Offline Verification of Aadhaar

ii. 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

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

v. The official of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

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

viii. Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the RE itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. Company are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Company.

xiii. Company shall ensure to redact or blackout the Aadhaar number.