Electronica Finance Limited

KYC & Anti-Money Laundering Policy

Version control:

Version No.	Description of change	Memorandum of Change	Proposed by	Approval date	Owner dept.
1	First	Introduction of Policy	-	-	-
2	Review and introduction of new policy	Changes arising from RBI notification	Compliance	26-06-2023	Credit & Operations
3	Regulatory changes	Regulatory changes	Compliance	29-05-2024	Credit & Operations

Contents

1. Background:

Reserve Bank of India has issued Master Direction- Know Your Customer (KYC) Direction, 2016 including comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and all NBFCs are required to ensure that a policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company

2. Definition:

i) **"Aadhaar number",** shall mean the Aadhaar number as defined in Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

ii) **"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**.**

iii) **"Identity"**, Identity generally means a set of attributes which together uniquely identify a "natural person "or a "legal person".

iv) **"Natural Person"**, A natural person's identity comprises his name and all other names used, the date of birth, and an address/location at which he/she can be located and also his/her recent photograph.

v) **"Legal Person"**, The legal status of the legal person/entity should be verified through proper and relevant documents; 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; understand the ownership and control structure of the customer and determine who are the natural person(s) who ultimately control the legal person. The identity of a legal/corporate person comprises its name, any other names it may use, and details of its registered office and business addresses.

vi) **"Beneficial Owner" ('BO')** shall have the meaning as per table below:

Sr. No.	Type of Customer	Beneficial Owners (BOs)
a	Public/Private Limited Companies	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 persons, has/have a controlling ownership interest or who exercise control through other means. Explanation- For the purpose of this sub-clause- 1. "Controlling ownership interest" means ownership of/entitlement to **more than 10 per cent** of the shares or capital or profits of the company. 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

Sr. No.	Type of Customer	Beneficial Owners (BOs)
b	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 **10 per cent of capital or profits** of the partnership. or who exercises control through other means. Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.
c	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	Trust	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.

Note: 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.

vii) "Certified Copy of OVD" or "Original Seen Verified (OSV)" - Obtaining a certified copy by the Company 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 authorized officer of the Company.

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

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

x) "Customer" for the purpose of this Policy would have the same meaning as assigned to it under the RBI's Guidelines on 'Know Your Customer' and Anti-Money Laundering Measures, as amended from time to time.

xi) "Customer Due Diligence (CDD)" means identifying and verifying the customer and the Beneficial Owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

xii) "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Company as per the provisions contained in the Act.

xiii) "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).

xiv) "Equivalent e-document" has been defined in Section 3 as 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.

xv) "**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.

Note: Customers where either of the following is done will not be treated as non-face-to-face customer:

1. Customer has walked in into any branch(es)/ office(s) of EFL for making application of loan.
2. Customer is met by authorized agent of EFL physically (e.g., DSA or its employee(s) or FCU vendor).
3. Customer is met by EFL employee physically.
4. Video KYC is done.

xvi) "Group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

xvii) "Non-profit organizations" (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

xviii) "Officially Valid Document" (OVD) means:

- the passport,
- the driving license
- 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.

Provided that,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof 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 license 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.*

Further, the Company can obtain following documents as a proof of Current/Present Address in addition to OVD:

1. Bank Statement (Not Older than 2 months at the time of Login)
2. Utility Bill (Not Older than 2 months at the time of Login)
3. Registered/ Notarized Rent Agreement
4. Index II/ Property Tax Receipt
5. Address on Employer Letter Head
6. Such other documents as may evidence as proof of Correspondence Address including but not limited to obtaining an undertaking signed by customer confirming correspondence address.

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

xx) **"The Company"** for the purpose of this Policy would mean Electronica Finance Limited.

xxi) **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

xxii) **"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).

xxiii) **"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), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xxiv) **"Principal Officer"** means an officer at the management level nominated by EFL, responsible for furnishing information as per rule 8 of the Rules.

The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

xxv) **"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 transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

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

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

xxviii) **"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.

xxix) **"Politically Exposed Persons" (PEPs)** are individuals who are or have been entrusted with prominent public functions in a foreign country, including Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

xxx) **"Designated Director"** means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the

Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the Company, if the Company is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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

The name, designation and address of the Designated Director shall be communicated to the FIU-IND. 14 (c) 26. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI. (d) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

3. Know Your Customer (KYC) Guidelines:

The Company's KYC Guidelines would include the following:

3.1 Customer Acceptance Policy

The Company shall have the following customer acceptance policy:

a. No account is opened in anonymous or fictitious/benami name.
b. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
c. No transaction or account-based relationship is undertaken without following the CDD procedure.
d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
e. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
f. 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.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

k. 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).

3.2 Guidelines on Unique Customer Identification Code (UCIC)

a) The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within the Company, across the banking system and across the financial system.

b) Unique identifiers for customers has been introduced within the Company. In our Company, Customer Code is the unique number assigned to customers. The CDD (Customer due diligence) procedure is applied at the UCIC level itself.

c) The existing customers having multiple Customer Codes are being consolidated by the exercise of deduplication.

d) While opening of a new account a unique code (only single Customer Code) for a customer will be allotted. Before allotting a new Customer Code to a customer, it shall be verified that the customer has not an existing Customer Code. If a customer has already one Customer Code, the new account(s) shall be tagged with the existing Customer Code.

e) The UCIC will also help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers.

3.3 Customer Due Diligence:

3.3.1 In case of an **Individual customer**, the Company shall obtain the following:

a. The proof of possession of Aadhaar number where offline verification can be carried out; or

b. The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or

c. the KYC Identifier with an explicit consent to download records from CKYCR

d. PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; or

e. Such other documents including in respect of the nature of business and financial status of the Customer, or the equivalent e-documents thereof as may be required by the Company:

Provided that where the customer has submitted:

i) proof of possession of Aadhaar as above where offline verification can be carried out, the Company shall carry out offline verification;

ii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take a live photo as specified under **Annexure II – Digital KYC**; and

iii) any OVD or proof of possession of Aadhaar number as above, where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under **Annexure II – Digital KYC**.

iv) the Company shall retrieve the KYC records online from the CKYCR.

Offline verification of Aadhaar can be accomplished by two means: Via the QR code on Aadhaar card & E-Aadhaar PDF.

By downloading Offline Aadhaar file (a password protected ZIP file containing an XML file) from UIDAI's website which shall be verified through OTP sent to the mobile number of the customer.

Detailed process for carrying out offline verification of Aadhaar is listed at **Annexure III**.

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

The Company shall, where its customer submits a proof of possession of Aadhaar containing Aadhaar Number, **ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required.**

3.3.2 In the case customer **is a Sole proprietorship firms**, CDD of proprietors shall be carried in the same manner as provided above. In addition to the above **any of the following two documents or equivalent e-documents as a proof of business/ activity in the name of the proprietary firm** shall also be obtained:

a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
b) Certificate/license issued by the municipal authorities under Shop and Establishment Act
c) Sales and income tax returns
d) CST/VAT/ GST certificate
e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
f) 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
g) Utility bills namely electricity/ water/ landline/ telephone bills issued in the name of the firm.
h) Importer Exporter Code (IEC) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
i) In cases, where it is not possible to furnish any two of the above documents, the Company may accept any one of above stipulated document subject to field verification done for the proprietorship firm.

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.

3.3.3 In case customer **is a company**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

a) Certificate of incorporation;
b) Memorandum and Articles of Association;
c) PAN of the company;
d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and

e) Documents, of beneficial owner, the managers, officers, or employees, as the case may be, holding an attorney to transact on the company's behalf in the manner as mentioned in the Policy.
f) the names of the relevant persons holding senior management position; and
g) the registered office and the principal place of its business, if it is different.

3.3.4 In the case of firms reconstituted and the companies that changed the name within the past two years, the CDD would be enhanced.

3.3.5 In case customer **is a partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
a) Registration certificate as proof of registration of the firm;
b) Partnership deed;
c) PAN of the partnership firm;
d) Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the Policy.
e) the names of all the partners and
f) address of the registered office, and the principal place of its business, if it is different.

3.3.6 In case customer **is a Trust**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
a) Registration certificate;
b) Trust deed;
c) Permanent Account Number or Form No.60 of the trust; and
d) Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the Policy.
e) the names of the beneficiaries, trustees, settlor and authors of the trust
f) the address of the registered office of the trust; and
g) list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorized to transact on behalf of the trust.

3.3.7 In case customer **is an unincorporated association* or a body of individuals****, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
a) Resolution of the managing body of such association or body of individuals;
b) PAN or Form No. 60 of the unincorporated association or a body of individuals;
c) Power of attorney granted to transact on its behalf;
d) Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the Policy; and
e) Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

*Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

**Term 'body of individuals' includes societies.

3.3.8 For opening accounts of **juridical persons** not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:
a) Document showing name of the person authorized to act on behalf of the entity;
b) Documents, as specified in Section 16, of the person holding an attorney to transact

on its behalf; and

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

3.3.9 For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of 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
   (i) an entity listed on a stock exchange in India, or
   (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
   (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

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.

3.3.10 For all the customers irrespective of the risk categorization, the Company would undertake following customer acceptance procedure:

a) Internal dedupe - Checking the internal records of the Company to confirm about any past dealings of the customer with the Company either as borrower, co-borrower or guarantor;

b) External dedupe – Verifying with the data base maintained by at least one RBI approved credit information bureau;

3.3.11 Proof of possession of Aadhaar number (with specific consent of the customer) and copy of the PAN Card (Form 60 in case the Customer does not have a PAN) shall be obtained from all new individual customers (from each party to the Agreement) and authorized Signatory of Legal Entity while establishing an account-based relationship.

3.3.12 In case 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 certified copy/OSV of an OVD containing details of identity and address and one recent photograph shall be obtained.

3.3.13 The documents to be obtained from Individual not eligible to be enrolled for an Aadhaar, or a person who is not a resident shall be PAN or Form 60 (in case the Customer does not have a PAN), as amended from time to time, one recent photograph and certified copy/OSV of OVD containing details of identity and address.

3.3.14 The System should be in place to capture Customer classification from the Money Laundering perspective including flagging of negative profile customers, terrorist organizations as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) etc.

3.4 Customer Identification Procedure -

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

a. Commencement of an account-based relationship with the customer.
b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. Selling third party products as agent

3.4.2 Customer identification means identifying the customer and verifying his / her identity

by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami person.

3.4.3 The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

3.4.4 An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

a. Verify the identity of any Person transacting with the Company to the extent reasonable and practicable

b. Maintain records of the information used to verify a customer's identity, including name, address and other identifying information and

c. Consult sanctions lists/ FATF statements of known or suspected terrorists:

The Company shall ensure that, in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, the Company 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) and whose names appears in the two sanctions lists circulated by RBI. The details of sanction lists circulated UNSC are as under:

i) ISIL (Da'esh) & Al-Qaida Sanctions List

ii) Taliban Sanctions List

The Company may ensure the aforesaid, verifying the name of person or entity through the website of the concerned entity or through the service provider, who provide the said service of third party verification, in compliance applicable provisions/guideline of Reserve Bank of India, the Prevention of Money Laundering Act and rules made thereunder in this regard.

Details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list, shall be treated as suspicious and reported to the FIU-IND, apart from advising Ministry of Home Affairs as required under UAPA notification.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing.

The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

3.4.5 For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Company, shall at their option, rely on customer due diligence done by a 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 from the third party or from the Central KYC Records Registry.

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

c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PMLA.

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.

3.4.6 The Company may carry out Video based Customer Identification Process (V-CIP) as a consent based alternate method of establishing the customer's identity, for customer onboarding. V-CIP shall be carried out in the manner provided in the **Annexure II** of this Policy.

3.5 Risk Management -

3.5.1 The following elements would manage the Risk arising out of the non-compliance to PMLA:

a) The Board will ensure that an effective KYC program is put in place by establishing appropriate procedures and ensure their effective implementation.
b) All the Customers would be classified under three heads viz. Low Risk, Medium Risk and High Risk. Refer Annexure - I for risk categorization of customers.
c) The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds. The extent of monitoring shall be aligned with the risk category of the customer.
d) The Company would have an on-going employee training program with different focuses for frontline staff, compliance staff and staff dealing with new Customers and educating them with respect to the objectives of the KYC Program.
e) Periodical updating of Customer identification data would be taken up once in **ten years** for low-risk Customers, once in **eight years** for medium risk Customers and once in **two years** for high-risk Customers as per the following procedure:

3.5.2 The Company shall carry out:

a) CDD at the time of periodic updation. However, 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.
b) In case of Legal entities, the Company shall review the documents sought at the time of opening of account and obtain fresh certified copies.

3.5.3 The Company shall ensure to maintain record along with date of KYC updation in Companies records.

3.5.4 On-going due diligence

a) The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.
b) Without prejudice to the generality of factors that call for close monitoring, following types of transactions if applicable, shall necessarily be monitored:
    i) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
    ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.
    iii) High account turnover inconsistent with the size of the balance maintained.
    iv) Deposit of third-party Cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts. For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.
c) The extent of monitoring shall be aligned with the risk category of the customer.

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

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

ii) The transactions in accounts of marketing firms, especially accounts of Multi-Level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of Cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

3.5.5 Updation / Periodic Updation of KYC

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.

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, 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, 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, as defined in Section 3(a)(xiii), 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 Legal Entities (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Company, digital channels (mobile application of the 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:

The Company shall also ensure that,

i. The KYC documents of the customer as per the current CDD standards are available with them. 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. The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Company's end.

3.5.6 A Chief Compliance Officer (CCO) would be designated as the Principal Officer – PMLA and would report to senior management. The Principal Officer – PMLA would perform the following duties:

a) Develop effective Anti-Money Laundering programs, including training programs.
b) Assist business in assessing how the System can be abused.
c) Identify suspicious activity.
d) Monitor implementation of this Policy.
e) Submit reports to statutory bodies, management and maintain liaison.
f) Ensure verification of KYC/ AML compliance by the front desk staff/officers.

3.5.7 Internal audit, compliance and risk function would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

3.5.8 Concurrent/ Internal Auditors should 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 would be put up before the Audit Committee of the Board on quarterly basis.

3.6 Transaction monitoring -

3.6.1 The Company would continue to maintain proper record of all cash transactions of Rs.10 Lakh and above and have in place centralized internal monitoring system at head office. The Company shall obtain copy of Aadhaar Card and PAN of all the Customers for cash transaction of Rs. 50,000/- or more entered into with them. In case a Customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

3.6.2 For cash deposits of Rs 50,000/- or more made by any Third Party on behalf of the customer, an Authorization letter and self-attested PAN of the customer (in case the Customer does not have a PAN, Form 60 in lieu thereof) along with an I.D. proof of the person depositing the cash shall be obtained.

3.6.3 During sale of Repossessed assets, copy of the PAN Card or Form 60 (in case the Customer does not have a PAN), shall be obtained from the buyer of the vehicle in case the consideration amount is in excess of Rs. 50,000/- and is being paid in cash.

3.6.4 The Company would strive to have an understanding of the normal and reasonable activity of the Customer through personal visits and by observing the transactions and conduct of the account in order to identify transactions that fall outside the regular pattern of activity – unusual transactions.

3.6.5 For the simplicity of data capture, the following transactions would be considered as unusual transactions deserving special attention. Such accounts would be treated as Medium/ High Risk Customers after review of the unusual transactions by the Principal Officer – PMLA.

- Repeated pre-termination of loan accounts of size exceeding Rs.10 lacs;
- Same Customer appearing in the Cash Transaction Report (CTR) more than 3 times during a span of 6 months; and
- Total cash received from a customer exceeding Rs 50 lacs in a financial year or Rs. 25 lakhs in a month.

3.6.6 Being an NBFC, the Company is not empowered to seize any counterfeit currency like in the case of banks. However, the following incidents of counterfeit currency at the cash counters would be recorded and repeated occurrence would be reported.

- Bulk counterfeit currency of more than 10 pieces at a time; and
- Repeated event within a week from a collection executive or Customer.

3.6.7 All such transactions would be reported to and reviewed by Principal Officer – PMLA who would enquire into the matter and decide whether the transaction would qualify to be termed as a suspicious transaction. When it is believed that we no longer are satisfied that we know the true identity of the account holder, STR would be filed with FIU-IND. The Principal Officer - PMLA would file the Suspicious Transaction Report (STR) with the Director, Financial Intelligence Unit-India (FIU-IND) within 7 (seven) days of identifying them. After filing STR, transactions would be allowed to be continued in the account unhindered and the Customer would not be tipped in any manner.

3.6.8 All CTR/ STR would be filed electronically or as per the norms stipulated by FIU-IND from time to time. The STR would be filed even for attempted transactions.

3.6.9 List of individuals and entities, approved by UN Security Council Committee and circulated by RBI would be updated and the list would be available at every office entrusted with the responsibility of customer acceptance and would be verified before opening an account. Financial Action Task Force (FATF) statements regarding countries with deficient AML/CFT would be verified and caution would be exercised with Customers who conduct business activities in these countries.

3.6.10 The Company has a laid down Document Retention policy which would be reviewed periodically to be in compliance with the requirements of PMLA. The following documents/records would be held for a period of 10 years:

- Records with respect to the cash transactions of value of more than Rs. 10 lacs;
- Records with respect to series of cash transactions integrally connected to each other of more than Rs.10 lacs within a month;
- Records with respect to transactions where counterfeit currency notes have been used;
- Records with respect to all suspicious transactions; and
- KYC documents after the business relationship ending.

3.6.11 The documents/ records maintained would hold the following information:

- Nature of transaction;
- Amount of the transaction;
- Date on which the transaction was conducted; and
- The parties to the transaction.

3.6.12 All the units reporting the unusual transactions to Principal Officer – PMLA would be subjected to audit by the Internal Audit Department.

3.7 Enhanced Due Diligence

Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.
Following EDD measures shall be undertaken by REs for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

a) In case the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
c) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
d) The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

3.8 Accounts of Politically Exposed Persons (PEPs)

The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) (subject to the restriction mentioned in credit policies for various products) provided that apart from performing normal customer due diligence:

a) The Company have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP
b) Reasonable measures are taken by the Company for establishing the source of funds / wealth
c) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
d) the identity of the person shall have been verified before accepting the PEP as a customer;
e) the approval to open an account for a PEP shall be obtained from the senior management;
f) all such accounts are subjected to enhanced monitoring on an on-going basis;
g) 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;
h) the CDD measures as applicable to PEPs including enhanced monitoring on an on- going basis are applicable
i) The mandatory information to be sought for KYC purpose while opening an account is

specified.

j) Circumstances in which, a customer is permitted to act on behalf of another person/ entity, is clearly spelt out.

k) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

l) The above instructions shall also be applicable to accounts where a PEP is the beneficial owner and shall also be applicable to family members or close associates of PEPs.

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

a) The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, RBI KYC Master Directions issued from time to time, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.

b) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 of RBI- Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on May 10, 2021) (RBI KYC Directions) or as per Section 18 (V-CIP) of Chapter VI, Part I - Customer Due Diligence (CDD) of RBI KYC Directions- Procedure in case of Individuals is carried out, If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

c) 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.

d) The Company shall upload KYC records pertaining to accounts of Legal Entities opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules. 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) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/ update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/ received from the customer.

g) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to a Company, with an explicit consent to download records from CKYCR, then such 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 –

- there is a change in the information of the customer as existing in the records of CKYCR;
- the current address of the customer is required to be verified; and
- 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 Customer.
- the validity period of documents downloaded from CKYCR has lapsed.

5 Important provisions under PMLA:

5.3 The offense of money laundering is defined as "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering".

5.4 Punishment for Money Laundering is laid down as "whoever commits the offense of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but may extend to seven years and shall also be liable to

fine which may extend to five lakh rupees".

5.5 The Company shall:

a) Maintain a record of all transactions the nature and value of which may be prescribed, whether such transaction comprise of a single transaction or series of transactions integrally connected to each other and where such series of transactions take place within a month.

b) Furnish information of transactions referred to in the clause above to the Director (FIU-IND) within such time as may be prescribed.

c) Verify and maintain records of the identity of all its clients, in such a manner as may be prescribed.

d) Identify Beneficial Owner, if any, of such of its clients, as may be prescribed.

e) Maintain record of documents evidencing identity of its clients and Beneficial Owners as well as account files and business correspondence relating to its clients.

f) Where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director-FIU IND within the prescribed time.

g) The records referred to above shall be maintained for a period of ten years from the cessation of the transactions between the clients and the banking company of financial institution or intermediary, as the case may be. However, details furnished to Director FIU-IND, documents related to identity and Beneficial Owner of the client shall be maintained permanently.

h) The reporting entities shall have "Designated Director" designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules thereof. The Designated Director can be any one of the Managing Director or a whole-time Director. However, in no case, the principal officer shall be nominated as the "Designated Director" for the purpose of this Policy. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

i) The Director-FIU IND may whether on his own or on an application made by an authority, officer or person call for records referred to above and may make such inquiry or cause such inquiry to be made, as he thinks fit, with respect to obligations of the reporting entity.

5.6 If the Director-FIU IND, in the course of any inquiry, finds that a banking company, financial institution or intermediary or any of its officers has failed to comply with the provisions for maintenance of records, furnishing of information, verification of identity of customers etc., then without prejudice to any other action that may be taken under any other provisions of PMLA, Director – FIU-IND may, by an order, levy a fine on such banking company or financial institution or intermediary which shall not be less than ten thousand rupees but may extent to one lakh rupees for each failure.

6 Reporting of information with the FIU-IND:

The Company will make necessary arrangements from time to time to ensure compliance with the various reporting requirements as per the RBI's Guidelines on "Know Your Customer" and Anti-Money Laundering Measures or any other applicable law in force.

7. Implementation of KYC Policy

The Company has adopted various provision of KYC as per RBI Directives. However, the technology based KYC procedures will be implemented in due course as per technology road map and system development life cycle of respective technology enablers.

8. Review and Amendment in the Policy:

The Board of Directors shall review and amend this Policy and the risk categorization parameters forming the part of said policy; in the event of any update/ changes pursuant to amendments in RBI's KYC master direction, or any business requirements subject to applicable regulations and the Policy shall be reviewed at least annually.

ANNEXURES

Annexure I - Risk Categorization

1. **Risk parameters for risk categorization of customers**

   For **High-Risk** Customer application, revised KYC Document need to be collected in **every 2 years** from the date of Disbursal or from the date of last KYC Collected for all customers who are taken as Applicant/Co-Applicant/Guarantor on the Loan structure.

   For **Medium Risk** Customer application, revised KYC Document need to be collected in **every 8 years** from the date of Disbursal or from the date of last KYC Collected for all customers who are taken as Applicant/Co-Applicant/Guarantor on the Loan structure.
   For **Low-Risk** Customer application, revised KYC Document need to be collected in **every 10 years** from the date of Disbursal or from the date of last KYC Collected for all customers who are taken as Applicant/Co-Applicant/Guarantor on the Loan structure.

2. **Parameter of High-Risk Customer**

   While processing the application, if any customer on the loan structure falls under any of the below mentioned parameter, then application will be tagged as High Risk

   a) Politically exposed Persons (PEPs) as defined by RBI - customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
   b) Firms with sleeping partners - "Sleeping Partner" - A sleeping partner is a person who provides some of the capital for a business but who does not take an active part in managing the business. The same is some time specified in the Partnership Deed of the firm.
   c) Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff doesn't constitute physical presence.
   d) Client accounts managed by professional service providers such as law firms, agents, brokers, fund managers, trustees, custodians etc.
   e) Trusts, Charities, NGOs, Unregulated clubs and organizations receiving donations
   f) Customers that may appear to be multilevel marketing companies etc.
   g) Pawn brokers
   h) Real Estate Developers

3. **Parameter of Medium-Risk Customer**

   While processing the application, if any customer on the loan structure falls under any of the below mentioned parameter, then application will be tagged as Medium Risk

   a) Non-face-to-face customers are defined as customer who account is open without visiting Branch/Office or meeting EFL representative
   b) Non face-to-face application which are sourced through Website Sourced Cases, Call Centre, Loan Aggregators, Co-Lending, Direct Sales Sourced Cases (if not Met)
   c) Others Parameter irrespective of Face to Face or Non Face to Face souring
      - Dealers in high value or precious goods (eg. Jewel, gem and precious metal dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
      - Jewellers and Bullion Traders
      - Stock brokerage

4. **Parameter of Low-Risk Customer**

   While processing the application, if any customer on the loan structure falls under any of the below mentioned parameter, then application will be tagged as **Low Risk**

   a) All other profiles, Salaried individuals, Qualified Chartered Accountants, Doctors, Architects, Qualified Company Secretary, Cost Accountants
   b) All Other Profile not defined in High or Medium Risk Parameter
   c) Face to Face Customer where customer has either visited Branch/Office or met EFL representative i.e., Direct Sales Agent (DSA), FI Agency, EFL Employee Visit to customer place (Credit / Sales) / Customer walk-in (EFL Branch)

Annexure II – Video CIP and Digital KYC Process

Video-Customer Identification Process:

A) **The Company may undertake V-CIP to carry out -**

(i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, Company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28, apart from undertaking CDD of the proprietor.

(ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

(iii) Updation/Periodic updation of KYC for eligible customer.

B) **V-CIP Infrastructure: -**

(i) The Company should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

(ii) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

(vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-security event under extant regulatory guidelines.

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

C) **V-CIP Procedure: -**

(i) Each Company shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. 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 fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.

(vi) The authorized 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:

a) OTP based Aadhaar e-KYC authentication;
b) Offline Verification of Aadhaar for identification;
c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the Customer; and
d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi Locker Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16. 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 3 (three) days for usage of Aadhaar XML file/ Aadhaar QR code, Company shall ensure that the video process of the V-CIP is undertaken within 3 (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, Company shall ensure that no incremental risk is added due to this.

(vii) 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.

(viii) 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 Digi Locker.

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

(x) The authorized 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.

(xi) 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.

(xii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

D) V-CIP Records and Data Management: -

(i) The entire data and recordings of V-CIP shall be stored in system(s) located in India. Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this Policy, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved

Digital KYC Process:

i. 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.
ii. The access of the Application shall be controlled by the Company, 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 One Time OTP controlled mechanism given by Company to its authorized officials.
iii. 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.
iv. 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 of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
v. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color and no other person shall come into the frame while capturing the live photograph of the customer.

vi. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

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

viii. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

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

x. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

xi. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction- id/reference-id number to customer for future reference.

xii. The authorized officer of the Company shall check and verify that: - (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.

xiii. 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.

Annexure III - Process of Offline Verification

UIDAI has launched Aadhaar Paperless Offline e-KYC Verification to allow Aadhaar number holders to voluntarily use it for establishing their identity in various applications in paperless and electronic fashion, while still maintaining privacy, security and inclusion.

UIDAI provides a mechanism to verify identity of an Aadhaar number holder through an online electronic KYC service. The e-KYC service provides an authenticated instant verification of identity and significantly lowers the cost of paper based verification and KYC. However, this method of online e- KYC is not available to all agencies and may not be suitable due to some of the following reasons:

- Online e-KYC requires reliable connectivity.
- Agency needs to have technical infrastructure to call online e-KYC service and deploy devices (as necessary).
- The resident may need to provide biometrics for the online e-KYC.
- UIDAI maintains a record of the KYC request for audit purposes.

Advantages of Aadhaar Paperless Offline e-KYC Privacy:

- KYC data may be shared by the Aadhaar number holder directly without the knowledge of UIDAI.
- Aadhaar number of the resident is not revealed, instead only a reference ID is shared.
- No core biometrics (fingerprints or iris) required for such verification.
- Aadhaar number holder gets a choice of the data (among the demographics data and photo) to be shared.

Security:

- Aadhaar KYC data downloadable by Aadhaar number holder is digitally signed by UIDAI to verify authenticity and detect any tampering.
- Agency can validate the data through their own OTP/Face Authentication.
- KYC data is encrypted with the phrase provided by Aadhaar number holder allowing residents control of their data.

Inclusion:

- Aadhaar Paperless Offline e-KYC is voluntary and Aadhaar number holder driven.
- Any agency working with people can use it with consent of the Aadhaar number holder allowing wide usage.

Aadhaar Paperless Offline e-KYC eliminates the need for the resident to provide photocopy of Aadhaar letter and instead resident can download the KYC XML and provide the same to agencies wanted to have his/her KYC. The agency can verify the KYC details shared by the resident in a manner explained in below sections. The KYC details is in machine readable XML which is digitally signed by UIDAI allowing agency to verify its authenticity and detect any tampering. The agency can also authenticate the user through their own OTP/Face authentication mechanisms.

How to obtain Aadhaar Paperless Offline e-KYC Data:

Aadhaar number holders can obtain Aadhaar Paperless Offline e-KYC data through the following channels:

- (https://resident.uidai.gov.in)
- In future, obtain Aadhaar Paperless Offline e-KYC will also be available via:
  - m-Aadhaar mobile application on a registered phone number
  - Inbound SMS using registered phone number
  - Aadhaar Kendra using Biometric Authentication

---------End of the Policy---------