ardent capital pvt ltd

KNOW YOUR CUSTOMER (KYC) AND PREVENTION OF MONEY LAUNDERING ACTIVITY POLICY.

Prepared by: Secretarial Department

Approved by: Board of Directors

Purpose: Created and Amended from time to time, pursuant to the Master Guidelines – Know Your Customer (KYC) guidelines 2016, PML Act, 2002 and the PML Rules, 2005.

CHAPTER – I

01. Introduction

Ardent Capital Private Limited ("Company") is a non-banking finance company ("NBFC") categorised as a non-deposit taking and non-systemically important NBFC company engaged in the business of providing loans and advances.

The policy set out herein has been approved by the Company's Board of Directors pursuant to the Reserve Bank of India ("RBI") Master Circular on "Know Your Customer – KYC guidelines", as amended from time to time. It is called Know Your Customer (KYC) & Anti-money Laundering (AML) Policy of the Company.

02. Objectives

The Reserve Bank of India has been issuing guidelines in regard to Know Your Customer (KYC) standards to be followed by banks and NBFCs and measures to be taken in regard to Anti Money Laundering (AML)/ Combating Financing of Terrorism (CFT). NBFCs are required to put in place a comprehensive policy framework, duly approved by the Board of Directors or competent authority authorized by Board of Directors, in this regard, this policy document has been prepared in line with the RBI guidelines and PMLA act and PMLA Rules.

03. Regulatory Requirement

We are required to follow certain customer identification procedure while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions.

The KYC policy shall include following four key elements:

1. Customer Acceptance Policy;
2. Risk Management;
3. Customer Identification Procedures (CIP); and
4. Monitoring of Transaction

04. Definitions: -

In this policy terms herein shall bear meaning as assigned in RBI Master Direction on KYC and/or other regulations as prescribed by Reserve Bank of India and meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

1. **"Aadhaar number"**, as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth 'The Aadhaar Act', means an identification number issued to an individual by Unique Identification

Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. **Aadhaar will be the document for identity and address.**

2. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

3. **Beneficial Owner (BO)**

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

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership.

Explanation- For the purpose of this sub-clause-

i) "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

ii) "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.

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

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

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

4. **Certified Copy**

Certified copy means comparing the copy of the proof of possession of Aadhaar Number where offline verification cannot be carried out or officially valid documents so produced by

the customer with the original and recording the same on the copy by the authorised officer of Company as per the provisions contained in the Act.

Provided that in case of Non-Resident Indian (NRI) & Persons of Indian Origin (PIOs) as defined in Foreign Exchange Management (Deposit) Regulations; 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.

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

6. **"Designated Director"** means a person designated and to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors.
7. **Digital KYC** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act.

8. **Digital Signature** shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
9. **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.

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

11. **"Non-profit organisations**" (NPO) means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

12. **"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).

13. "**Principal Officer"** means an officer nominated and responsible for furnishing information as per rule.

14. **Officially Valid Document** (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

- 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.
- 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: -
    - utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
    - property or Municipal tax receipt;
    - pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
    - letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

- the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- 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.

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.

15. **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).

16. **"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.

17. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
    (a)
    i. opening of an account;
    ii. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
    iii. the use of a safety deposit box or any other form of safe deposit;
    iv. entering into any fiduciary relationship;
    v. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

vi. Establishing or creating a legal person or legal arrangement.

(b) Terms bearing meaning assigned in this POLICY, unless the context otherwise requires, shall bear the meanings assigned to them below:

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

ii. "Walk-in Customer" means a person who does not have an account based relationship but undertakes transactions.

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

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: 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. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control; 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.]

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

19. **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest?

20. **"IGA"** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

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

22. **"Non-face-to-face customers"** mean customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

23. **"Video based Customer Identification Process (V-CIP):"** an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

24. **Wire transfer** related definitions:

a) **Batch transfer**: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.

b) **Beneficiary:** Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.

c) **Beneficiary Company:** It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary RE and makes the funds available to the beneficiary.

d) **Cover Payment:** Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

e) **Cross-border wire transfer**: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

f) **Domestic wire transfer**: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.

g) **Financial Institution**: In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.

h) **Intermediary Company**: Intermediary Company refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire

transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

i) **Ordering Company**: Ordering Company refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

j) **Originator**: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

k) **Serial Payment**: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).

l) **Straight-through Processing**: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

m) **Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

n) **Wire transfer:** Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

25. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers" profile and source of funds.

26. **"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.

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

28. Ardent Capital Private Limited is referred as NBFC-ND

29. **Common** Reporting **Standards (CRS)** means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II

05. DESIGNATED DIRECTOR & PRINCIPAL OFFICER

As required as per the KYC Guidelines and Policy of the Company, ***"Mr. Sivaraman Sudhakar"*** of the Company nominated by the Board shall act as Designated Director for the purpose of ensuring all the compliance with the obligations imposed under the Chapter VI of the PML act and the rules.
As Nominated by the Board, ***"Mr. Na S Jeyagar"*** shall act as Principal Officer who will be ensuring compliance, monitoring transactions, and sharing and reporting information as required under the laws and regulations.

06. Customer Acceptance Policy – Compliance

The Company shall frame policy duly approved by the Board of the Company

(A)Compliance of KYC policy

(a) Specifying as to who constitute, Senior Management" for the purpose of KYC compliance.

(b) Allocation of responsibility for effective implementation of policies and procedures.

(c) Independent evaluation of the compliance functions of REs" policies and procedures, including legal and regulatory requirements.

(d) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.

(e) Submission of quarterly audit notes and compliance to the Audit

(f) Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

(B) Customer Acceptance Policy

The Following norms and procedures will be followed by the Company in relations to its customer who approach the Company for availing services from the Company.

- No Account will be opened in anonymous or fictitious/benami name. Company shall ask for the sufficient Identity proof to proceed with the acceptance.
- No Account shall be opened in case of Company unable to apply the Customer Due Diligence 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.
- No transaction or account-based relationship will be undertaken without following the CDD measures.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- Whenever any additional information, which is not required as per the KYC Policy, shall be obtained with the explicit consent of the Customer.
- The Company shall apply the CDD procedure at the UCIC level. Therefore, in case where an existing customer of Company desire to open another account or avail any other product or services from the same Company, there shall be no need for fresh CDD exercise as far as identification of the customer is concerned.
- The Company shall follow the CDD procedure for all joint account holders, while opening a joint account.
- Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- Suitable system will be 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 indicated in chapter IX of the RBI master directions (Requirements/obligations under International Agreements - Communications from International Agencies).
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- 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).
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

- Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

The Company shall ensure the compliance of the above policy while keeping in mind that the same shall not result in denial of services to general public, especially those, who are financially or specially disadvantaged.

07. Risk Assessment and Management

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

A. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception and based on broad principals as laid down by Board of the company.
B. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity,
C. Company' policy framework should seek to ensure compliance with PML Act/Rules, including Company regulatory instructions in this regard and should provide a bulwark against the threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, Company may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.
D. Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Company from time to time.
E. The risk assessment by the Company shall be properly documented and be proportionate to the Company, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

G. Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedure in this regard. Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Company shall monitor the implementation of the controls and enhance them if necessary.

H. Information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

I. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

J. That various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: *FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.*

08. Customer Identification Procedure (CIP)

"Customer identification" means undertaking the process of CDD.

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

The company shall undertake identification of customers in the following cases:

- Commencement of an account-based relationship with the customer.
- When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

- Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- When the company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

09.Customer Due Diligence Procedure

The Company may rely on the customer due diligence done by a third party for the purpose of verifying the identity of customers at the time of commencement of an account based relationships, subject to the following conditions;

- Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
- 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.
- The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

Part I - CDD Procedure in case of Individuals

For undertaking CDD, Company shall obtain the following 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:

The Company shall obtain the following documents when the customer is an **Individual;**

No,	Name of the Documents	Further Details /Explanation
1	Aadhaar Number	➢ Aadhaar Number where 1. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

		2. he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or ➢ the proof of possession of Aadhaar number where offline verification can be carried out; or ➢ 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 ➢ the KYC Identifier with an explicit consent to download records from CKYCR;
2	PAN Number	➢ the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962
3	Such Other Documen	➢ documents with 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:

In Case a person who desires to open an account is not able to produce the above documents, the Company may at its discretion open accounts with the following documents;

No,	**Name of the Documents**	**Further Details**
01	Photograph	A Self-attested photograph from the customer.
02	Certified copy of Officially valid documents (OVD)	Officially Valid documents includes; Passport Driving licence Proof of possession of Aadhaar Number Voter's Identity Card Job Card issued by NREGA duly signed by State Govt. Officer Letter issued by the National Population Register containing details of name and address.
03	In case the OVD Documents provided not having the updated address may asked for additional documents	The Following documents shall be deemed to be OVDs for the limited purpose of Proof of Address: - 1. Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); 2. Property or Municipal Tax receipt;

		3. Bank account or Post Office savings bank account statement; 4. Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; 5. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, and public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and 6. Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.
04	Such Other Documents	documents with 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:

- Aadhaar number under clause (a) above to a bank or to a Company notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data repository, he may give a self-declaration to that effect to the Company.
- proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.
- an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC
- KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR.

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 of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit as mandated in paragraph 8. Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Company and shall be available for supervisory review.

Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

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

- The customers shall not be required to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address.
- The account shall remain operational initially for a period of twelve months, within which CDD as required shall be done by the Company.
- where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required by the Company.
- The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

The Company may undertake live Video Customer Identification Process (V-CIP) by the authorised person of the Company after getting the consent of the customer. The guidelines *to carry V-CIP is given in the Annexure C of this policy.*

OTP Based e-KYC, in non-face to face mode: -

Provided further that the company may provide an option for One Time Pin (OTP) based e-KYC process for on-boarding of customers. Accounts opened in terms of this proviso i.e., using OTP based e-KYC, are subject to the following conditions:

(i) There must be a specific consent from the customer for authentication through OTP;

(j) As a risk-mitigating measure for such accounts, Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Company shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile

(ii) Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year. Account should not allow for more than one year.

(iii) Borrower accounts opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure is to be completed. If the CDD procedure is not completed within a year, no further debits shall be allowed.

(iv) 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 either with the company or with any other RE. Further, while uploading KYC information to CKYCR, the 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.

(v) The company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

The company shall print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal, if such a customer knows only his/her Aadhaar number or if the customer carries only a copy of Aadhaar downloaded from a place/source elsewhere, provided, the prospective customer is physically present in the branch of the RE.

A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the „officially valid document" in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

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 company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation and a self-declaration from the account holder about his/her current address is obtained in such cases.

Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs): In case a person who desire to open an account is not able to produce documents, as specified in paragraph 16, NBFCs may at their discretion open accounts subject to the following conditions:

(a) The Company shall 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 per paragraph 16 or paragraph 18 shall be carried out.

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

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

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

(g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

(h) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per paragraph 16 or paragraph 18.

(i) 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.

(j) Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

Part II - CDD Measures for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, a certified copy of an OVD as mentioned above, containing details of identity and address of the individual (proprietor) shall be obtained.

In addition to the above, any two of the following documents as a proof of Business/ activity in the name of the proprietary firm shall also be obtained:

a. Registration certificate including Udyam registration Certificate (URC) issued by the Government

   Notwithstanding the provisions given above, in respect of an individual customer who is categorized as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The Company shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

b. Certificate/licence 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. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / License /certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
h. Utility bills such as electricity, water, and landline telephone bills.

In cases where the company is satisfied that it is not possible to furnish two such Documents, company may, at its 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.

Part III- CDD Measures for Legal Entities

Certified copies of each of the following required in case of;			
A Company	**A Partnership Firm**	**A Trust**	**An unincorporated association or a body of individuals.**
➢ Certificate of Incorporation; ➢ Memorandum and Articles of Association; ➢ PAN of the Company; ➢ A resolution of Board of Directors and Power of Attorney granted to its manager, directors, officers or employees to transacts on behalf; ➢ Documents of an Individuals as referred in Part I of beneficial owner; ➢ The names of the relevant persons holding senior management position; ➢ The registered office and the principal place of its business, if it is different.	➢ Registration Certificate ➢ Partnership deed ➢ PAN of Partnership firm ➢ Documents of an individual as referred in Part I of the beneficial owner, managers, officers, employee, as the case may be, whose holding an attorney to transacts on its behalf; ➢ The name of all the partners; ➢ Address of the registered officer and the principal place of business, if it's different.	➢ Registration Certificate ➢ Trust Deed ➢ Pan of Trust ➢ Documents of an individual as referred in Part I of the beneficial owner, managers, officers, employee, as the case may be, whose holding an attorney to transacts on its behalf; ➢ Name of the beneficiaries, trustee, settlor, protector if any and authors of the trust ➢ Address of the registered office ➢ List of documents of individual who discharging the role as trustee and authorised to transact on behalf	➢ Resolution of the managing director ➢ PAN or Form No. 60 ➢ Power of Attorney granted to transact on its behalf ➢ Documents of an individual as referred in Part I of the beneficial owner, managers, officers, employee, as the case may be, whose holding an attorney to transacts on its behalf; ➢ Such other information as required by the Company to establish its legal existence

Explanation: -

Unregistered trust and partnership firms shall be included under the term "unincorporated associations. The term "Body of Individuals" includes societies.

A customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such

juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

- Document showing name of the person authorised to act on behalf of the entity
- Documents of the individual as specified in Part I of the person holding an attorney to transact on its behalf and
- Such other documents as required by the company to establish its legal existence.

Provided that in case of a trust, the RE shall ensure that trustees disclose their status at the time of commencement of an account-based relationship.

Part IV - Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps to verify his/her identity shall be undertaken keeping in view the following:

- 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.
- 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.

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/wealth.

Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- ⇨ 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.
- ⇨ Transactions which exceed the thresholds prescribed for specific categories of accounts.

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

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

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

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

Part V- On going Diligence

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.

Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

Periodic Updation

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 subject to the following conditions:

Type of Customer	**Periodic Updation**	
High Risk Customer	Once in Every 2 years	From date of opening of an account / last KYC Updation Notwithstanding the provisions given above, in respect of an individual customer who is categorized as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The Company shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.
Medium Risk Customer	Once in Every 8 years	
Low Risk Customer	Once in Every 10 years	

Periodic Updation for INDIVIDUAL	Periodic Updation for OTHER THAN INDIVIDUAL
In case of No change in KYC: A self-declaration from the customer in this matter shall be obtained through customer's email id registered with the Company, Mobile Number or any digital channel.	In case of No change in KYC: A self-declaration from the customer in this matter shall be obtained through customer's email id registered with the Company, Mobile Number or any digital channel. Letter from an authorised person of legal entities, Board resolution etc., as the case may be. Ensure that information of beneficial ownership available is up-to-date.
Change in Address: A self-declaration of the new address shall be obtained and the declared address shall be verified through positive confirmation within 2 months by means of such verification letters, contact point verification etc Further, the Company may at its discretion obtain a copy of OVD or deemed OVD for the proof of address as approved in their internal KYC Policy approved by the Board.	Change in Address: The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new legal entity customer. KYC documents as per the Current CDD standards must available with the Company. Documents/details received at time shall be promptly updated in the record of the company. Ensure compliance of Risk based approach, for requirement to see the KYC updation. The company may adopt the additional requirement of documents/details/ photograph etc.,
Customer who were minor, on becoming major: Fresh Photographs shall be obtained once become major. If required fresh CDD can be carry out	Others: The Company shall advice the customers 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.
Non-face to face node: KYC updation through OTP based e-KYC. If current address is different from address in aadhaar no positive confirmation required in this case.	

The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.	This shall be done within 30 days of the update to the documents for the purpose of updating the records at Company's end.

Change in KYC information:

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

(a) Fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorised as „low risk", when there is no change in status with respect to their identities and addresses and a self-certification to that effect is obtained.

(b) A certified copy of the proof of address forwarded by „low risk" customers through mail/post, etc., in case of change of address shall be acceptable.

(c) Physical presence of low risk customer at the time of periodic updation shall not be insisted upon.

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

(e) Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

(f) E-KYC process using OTP based authentication, for the purpose of periodic updation is allowed, provided, while on boarding, the customer was subjected to KYC process.

Additional measures: In addition to the above, Company shall 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, 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 115updation/ periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of 116updation/ periodic updation of KYC are promptly updated in

the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, Company may consider making available the facility of 117updation/ periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.

v. Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.

vi. 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 Company' end.

Due Notices for Periodic Updation of KYC

The Company shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, *inter alia*, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail. The Company shall expeditiously implement the same but not later than January 01, 2026.

In case of existing customers, Company shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, Company shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Company gives in writing to the Company that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this paragraph, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the provisions of this paragraph. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

Part VI - Enhanced and Simplified Due Diligence Procedure

The Company shall undertake the following EDD measures for;

EDD Measures for Non-face-face customer
➢ The Company shall include use of digital channels such as CKYCR, Digi Locker, equivalent e-documents etc. and non-digital modes such as obtaining OVD certified. ➢ The Company shall provide V-CIP as the first option to the customer for remote on boarding. ➢ The procedure of V-CIP shall be treated as par with face-to-face CIP for the purpose of KYC. ➢ Alternate Mobile Numbers shall not be linked post CDD with such accounts for Transaction OTP, updates etc., Transaction shall be permitted only from the mobile number used for account opening. ➢ The Company shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of register mobile number. ➢ Apart from obtaining the current address proof, RE 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. ➢ The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority. ➢ First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

- 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.

EDD Measures for Accounts of Politically Exposed Persons (PEPs)

The Company shall have the option of establishing a relationship with PEPs whether as customer or beneficial owner. Provided that.

- The Company have in place appropriate Risk management systems to determine whether the customer or beneficial owner is PEPs;
- Reasonable measures are taken by Company for establishing the source of funds/wealth.
- The approval to open an account for a PEP shall be obtained from the senior management.;
- All such accounts are subjected to enhanced monitoring on an on-going basis;
- 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.

These instructions shall also applicable to Family Members or close associates of PEPs.

Explanation: For the purpose of this paragraph, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions **by a foreign country**, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

EDD Measures for Accounts opened by Professional intermediaries

- The Company shall identify the client when such account has been opened by professional intermediary on behalf of a single client.
- The Company shall have an option to hold "pooled" accounts managed by professional intermediaries on behalf of an entities like mutual funds, pension funds or other types of funds
- The Company shall not open such accounts where professional intermediaries are bound by any client confidentiality that prohibits the disclosure of the client details to the Company.
- All the beneficial owners shall be identified where funds held by the intermediaries are not coo-mingled at the level of Company, and there are sub-accounts each of them attributable to a beneficial owner or where such funds are co-mingled at the level of Company, the Company shall look for the beneficial owners.

- The Company shall at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- The ultimate responsibility for knowing the customer lies with the Company.

CHAPTER – III

10. Record Management

10.1 Maintenance of Records: -

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

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

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

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

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

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

(i) the nature of the transactions;

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

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

(iv) the parties to the transaction.

(f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(g) Maintain records of the identity and address of their customer, and records in respect of transactions in hard or soft format.

Explanation: For the purpose of this paragraph, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

Company shall ensure that in case of customers who are non-profit organisation, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Company shall register the details on the DARPAN Portal. Company shall also maintain such registration records for a period of five years after the business relationship between the customer and company has ended or the account has been closed, whichever is later.

10.2 Preservation of Records: -

The Company shall maintain the above explained records as required under the provision of PMLA.

- The Company shall maintain the records with respect to record of the identity and address of all clients and beneficial owners obtained while on boarding and updated thereafter for a period of five years from the date of cessation of relationship.
- The Company shall maintain records of all transactions for a period of five years from the date of transaction.
- The Company shall preserve these records in such manner that it can be easily available upon the request of statutory authorities.

. Explanation: For the purpose of this paragraph, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

11. Reporting Requirement

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

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

The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting *entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic*

Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by the company which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of the company , whose all branches are not fully computerized, shall have suitable arrangement to call out the transaction details from branches

which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have *been made available by FIU-IND on its website* ***http://fiuindia.gov.in.***

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

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

12. Requirements/obligations under International Agreements Communications from International Agencies –

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

i) 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

Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Company shall register the details on the DARPAN Portal. Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

ii) The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at **https://www.un.**org**/securitycouncil/sanctions/1988/materials**

Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council resolutions) Order, 2007, as amended from time to time. The

aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of. ***Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967***

The procedure laid down in the UAPA Order dated August 27, 2009 (Annex I of RBI Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

13. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

(a) Annex III of this Master Direction). Company shall ensure meticulous compliance with the "ProceduCompany for Implementation of section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

(b) In accordance with paragraph 3 of the aforementioned Order, company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) 135In case of match in the above cases, Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) Company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, 2005, Company shall

prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

g) In case an order to freeze assets under section 12A is received by the Company from the CNO, Company shall, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities ', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council resolution on Democratic People's republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, Company shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.

Company shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

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

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

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

c. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all

d. Documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

CHAPTER – IV

14. Miscellaneous Requirement

14.1 Secrecy Obligations and Sharing of Information:

a. The company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the company and customer.

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

c. The exceptions to the said rule shall be as under:

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

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

Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

14.2 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, as required by the revised KYC templates prepared for Individuals and legal entities as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

b. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updation as specified in paragraph 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Company obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of

the PML Rules, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Company.

c. Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

d. For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

(i) there is a change in the information of the customer as existing in the records of CKYCR;

or

(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or

(iii) 145the validity period of downloaded documents has lapsed; or

(iv) the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

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

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

(a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login - -> My Account --> Register as Reporting Financial Institution,

(b) Submit online reports by using the digital signature of the „Designated Director" by either uploading the Form 61B or „NIL" report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: *The Company shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.*

(c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

(d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from Time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx JFIL may take note of the following:

a) updated Guidance Note on FATCA and CRS
b) a press release on "Closure of Financial Accounts" under Rule 114H

Account *payee* cheques for any person other than the payee constituent shall not be collected.

14.4 Collection of Account Payee Cheques

- A Unique Customer Identification Code (UCIC) shall be allotted while entering into new *relationships with individual customers as also the existing customers by the company.*
- *The company shall, at their option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions* with them and ensure that they are allotted UCIC.

14.5 Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, Company shall ensure:

(a) to undertake the ML/TF Money laundering / Financing of terrorism risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

14.6 Quoting of PAN : Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

14.7 Selling Third party products:

The company acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

(a) The identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand.

(b) Transaction details of sale of third party products and related records shall be maintained.

(c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:
- debit to customers" account or against cheques; and
- Obtaining and verifying the PAN given by the account based as well as walk-in customers.

(e) Instruction at „d" above shall also apply to sale of the company own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

14.8 Hiring of Employees and Employee training

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

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the company, regulation and related issues shall be ensured.

(c) Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

14.9 Adherence to Know Your Customer (KYC) guidelines by persons authorised by the company including brokers/agents etc.

(a) Persons authorised by the company for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to the company.

(b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by the company including brokers/agents etc. who are operating on their behalf.

(c) The books of accounts of persons authorised by the company including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection

Review of policy

Know Your Customer Policy may be reviewed annually. However, changes, if any, will be made in the Policy from time to time based on the changes in Regulatory and Statutory Guidelines, various laws including Prevention of Money Laundering Act, 2002 and RBI guidelines.
The Chief Executive Officer and / or Managing Director are authorized to approve/review of the KYC & AML Policy and modifications to the Policy from time to time.

Revisions made to the Policy

*policy being annually reviewed by the Board not included in the below table.

Versions	Date of Modification	Reviewed/ modified by	Approved by	Reason for modification
V1.0	02.03.2022	By Board of Director	Board of Directors in BM dated 02.03.2022	Creation and approval of the Policy
V2.0	08.05.2025	By Board of Director	Board of Directors in BM Dated 08.05.2025	Revised Pursuant to the RBI Amendments

ANNEXURES TO THE POLICY

ANNEXURE – A:

INDICATIVE LIST OF LICENCES/CERTIFICATES ISSUED IN THE NAME OF THE PROPRIETARY FIRM BY ANY PROFESSIONAL BODY INCORPORATED UNDER A STATUE

- Full Fledge Money Changer (FFMC) Licence issued by RBI.
- Small Scale Industries Certificate: Trade Licence issued by Department of Industries and Commerce.
- Permission issued by respective Government Authority for units in SEZ (Special Economic Zone), STP (Software Technology Park), EOU (Export Oriented Unit), EHTP (Electronic Hardware Technology Park), DTA (Domestic Tariff Area) and EPZ (Export Processing Zone).
- Registration Certificate of recognised Provident Fund with PF Commissioner.
- Permission to carry out business issued by Village Administrative Officer / Panchayat Head / Mukhiya/ Sarpanch / Talati / Village Developmental Officer / Block Development Officer or Equal Rank Officer for customers in rural / village areas and President / CEO if the document is issued by Nagar Parishad / Zilla Parishad. Branch to ascertain and ensure that the official who has signed the certificate has been empowered to do so.
- Factory Registration Certificate issued by any State / Central Government Authority.
- Licence to sell stock or exhibit for sale or distribute insecticides, under the Insecticides Rules, issued by respective State / Union Government Department.
- Licence issued under Contract Labour (Regular & Abolition) Act 1970. If generated online it should be attested by Municipal Authorities.
- Licence issued by Police Department under the provisions of State Police Acts.
- Zilla Udyog Kendra Registration Certificate.
- Registration for Fire Goods issued by Municipal Corporations.
- Trade Licence from Labour Department.
- Certificate issued by ANCHAL SAMITI MEMBER for existence of Firm. The Anchal Samiti exists at the Block level in Arunachal Pradesh and is a body under the Panchayati Raj system for a cluster of villages.
- APMC / Mandi License / Certificate and as part of due diligence, please obtain the receipt for amount paid to the concerned authority for issuance/ renewal of this license.
- Gram Panchayat Certificate (should be on letterhead and not more than 3 months old).

ANNEXURE – B

"DIGITAL KYC PROCESS"

- 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.
- 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 Time OTP controlled mechanism given by Company to its authorized officials.
- 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.
- 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.
- 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 colour and no other person shall come into the frame while capturing the live photograph of the customer.
- 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.
- The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- 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.
- Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature

on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. ***The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer***.

- 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.
- 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.
- 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.;
- 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 – C

VIDEO BASED CUSTOMER IDENTIFICATION PROCESS – (V-CIP)

The Company may undertake the Video based Customer Identification Process (V-CIP) for following scenarios;

1. For Customer Identification Process of new on-boarding customer
2. To carry out V-CIP for the updation/periodic updation of KYC of eligible customers.
3. Conversion of existing accounts opened in non-face to face mode using Aadhar OTP based e-KYC authentication.

Infrastructure Standard for V-CIP to be followed by the Company

- The Company shall comply with the RBI guidelines on minimum baselines cyber security and resilience framework, as updated from time to time.
- 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.
- No data shall be retained by the cloud service provider or third party technology provider assisting the V-CIP of the Company. All data shall be transferred to Company's exclusively owned server including cloud server.
- The Company shall ensure end-to-end encryption of data between customer device and the hosting point of V-CIP application.
- The Customer consent should be recorded in an auditable and alteration proof manner.
- The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- 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.
- 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 RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- 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-event under extant regulatory guidelines.
- 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 the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

- 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.

V-CIP Procedure to be followed by the Company: -

1. The Company shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it.
2. The V-CIP process shall be initiated by officials of the Company specifically trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.
3. Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.
4. 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.
5. Any prompting observed at end of customer shall lead to rejection of the account opening process.
6. 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 work-flow.
7. The authorised official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
    - ✓ OTP based Aadhaar e-KYC authentication;
    - ✓ Offline Verification of Aadhaar for identification;
    - ✓ KYC records downloaded from CKYCR, using the KYC identifier provided by the customer;
    - ✓ Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi Locker;

    Company shall ensure to redact or blackout the Aadhaar number.

8. 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 three working days from the date of carrying out V-CIP.
9. Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, Company shall ensure that the video process of the V-CIP is undertaken within three working

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.

10. 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.
11. 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.
12. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
13. The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
14. Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.
15. 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.
16. All matters not specified under the procedure here but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Company.

V-CIP Records and Data Management: -

The entire data and recordings of V-CIP shall be stored in a system / systems 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 MD, shall also be applicable for V-CIP.

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

*****