PIRAMAL ENTERPRISES LIMITED

POLICY ON KNOW YOUR CUSTOMER (KYC) / ANTI MONEY LAUNDERING (AML) / COMBATING THE FINANCING OF TERRORISM (CFT)

Dated: January 29, 2024

FOR INTERNAL USE ONLY

Policy owner:	**Compliance Department (Company-wide)**
Policy location:	**Mumbai, India**
Version:	**V 3- Review of Policy**
Approved on Date:	**January 29, 2024**
Approved by:	**Board**
Supersedes:	**V 2.0 (Review of Policy)**

I. Preamble

The Master Direction – Know Your Customer (KYC) Direction, 2016 issued by the Reserve Bank of India (RBI) has consolidated directions on Know Your Customer (KYC), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in line with the provisions of the Prevention of Money Laundering Act, 2002 (PMLA) and the rules therein as amended from time to time.

In view of the same, Piramal Enterprises Limited (PEL) referred in this document as the 'Company' has adopted the said KYC Master Direction with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures be formulated in line with the prescribed RBI guidelines and duly approved by its Board of Directors.

PEL will implement group-wide programs against money laundering and terror finance risk management across its subsidiaries. In addition, the Company will share information within its group companies as required for the purposes of client due diligence and AML/ KYC related information with adequate safeguards on confidentiality and safeguarding to prevent tipping-off.

II.Objectives, Scope and Applicability of the Policy

The objective of KYC & AML guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. The KYC / AML / CFT procedures will-will also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently.

The KYC / AML / CFT policy will include following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures (CIP);
c) Monitoring of Transactions; and
d) Risk Management

In addition, the Policy will also aim to achieve the following purposes:

i. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

ii. To comply with applicable laws and regulatory guidelines and take necessary action including application of additional measures to manage the Money Laundering (ML)/ Terrorist Financing (TF) risks.

iii. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures

iv. Provides management oversight on the KYC/AML/CFT compliance within the Company

v. Outline the requirements of training related to KYC/AML/CFT

III. Definition

"**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.

(i) Customer:

For the purpose of this Policy, a Customer is defined as a person, who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or the activity, is acting.

For the above definition, a Person means the below:

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 above persons (a to e); and
g) Any agency, office or branch owned or controlled by any of the above persons (a to f)

(ii) Beneficial Owner (BO):

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

   Explanation - For the purpose of this sub-clause:

   (i) "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the Company.

   (ii) "Control" will include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

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 percent of capital or profits of the partnership or who exercises control through other means.
   Explanation - For the purpose of this sub-clause, "control" will include the right to control the management or policy decision.

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 percent 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 or who purports to act on behalf of such juridical person or individual or trust,

d) Where the customer is a trust, the identification of beneficial owner(s) will include identification of the author of the trust, the trustee, the beneficiaries with 10 percent 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.

(iii) Central KYC Records Registry (CKYCR):

An entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

Certified Copy" –
Obtaining a certified copy by the Company will mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the Act.

(iv) Digital KYC:

It means 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.

(v) Digital Signature:

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

(vi) Equivalent e-document:

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.

(vii) Know Your Client (KYC) Identifier:

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

(viii) Suspicious transaction:

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.

(ix) Video based Customer Identification Process (V-CIP):

V-CIP is 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 Customer Due Diligence (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 will be treated on par with face-to-face CIP.

(x) Politically Exposed Persons (PEP):

"Politically Exposed Persons" are individuals, who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States or of governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

The terms not explicitly defined in this Policy, will draw reference to Para 3 from the Master Direction – Know your Customer (KYC Directions), 2016 issued by RBI.

IV. Customer Acceptance Policy

The guidelines for Customer Acceptance Policy (CAP) of the Company are as given below:

a) No account is to be opened in anonymous or fictitious/ benami name.

b) No account is to be opened where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non- cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company may consider filing a Suspicious Transaction Report (STR), if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer, basis evaluation by the Principal Officer (PO).

c) No transaction or account-based relationship is undertaken without following the CDD procedure.

d) The mandatory information as prescribed by the regulator from time to time will be sought for KYC purpose while opening an account and during the periodic updation.

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

The Company will apply the CDD procedure at the UCIC level. If an existing KYC compliant customer of the Company desires to open another account with the Company, no fresh CDD exercise will be undertaken.

f) CDD Procedure is followed for all the joint account holders, while opening a joint account.

g) Circumstances in which, a customer is permitted to act on behalf of another person/entity, will be to the satisfaction of the Chief Operating Officer/Chief Financial Officer/National Credit Manager of the Company/ Business Head.

h) To ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists issued by Reserve Bank of India, from time to time.

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

j) Where an equivalent e-document is obtained from the customer, the Company will verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

k) Where Goods and Services Tax (GST) details are available, the GST number willwill be verified from the search/verification facility of the issuing authority.

l) The Company can establish a relationship with PEPs (whether as customer or beneficial owner), as apart from performing normal customer due diligence:

(i) The Company has in place appropriate system to determine whether the customer or the beneficial owner is a PEP;

(ii) Reasonable measures will be taken by the Company for establishing the source of funds / wealth;

(iii) In case of Wholesale vertical (including CMML), an approval will be obtained from the senior management / sanctioning committee to open an account for a PEP;

(iv) In case of Retail loans, authority for opening/closing of accounts of politically exposed accounts should be exercised by one level above the authorized officer.

(v) All such accounts will be subjected to enhanced monitoring on an on-going basis.

(vi) 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;

V. Customer Identification Procedures

Customer identification means undertaking the process of CDD i.e., identifying the customer and the beneficial owner verifying his / her / its identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as PAN, Voter ID card / Passport / Officially Valid Documents, etc. necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Company will not insist for obtaining Aadhar except for those accounts intended to receive government subsidies /subvention or benefits under direct benefit transfer scheme of the Government. However, customer voluntarily producing Aadhar for the purpose of identification will be accepted by the Company.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, Company will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company will

i. verify the legal status of the legal person/ entity through proper and relevant documents

ii. verify that any person purporting to act on behalf of the legal person/entity is so authorized

and identify and verify the identity of that person.

Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure I.

The Company will undertake identification of customers in the following cases:

a) Commencement of an account-based relationship with the customer.

b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

c) As and when applicable, selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.

For the purpose of verifying the identity of customers and the beneficial owner at the time of commencement of an account-based relationship, the Company will, rely on Customer Due Diligence (CDD) done by a third party, subject to the following conditions:

(a) Records or the information of the customer due diligence carried out by the third party is obtained – immediately from the third party or from the Central KYC Records Registry.

(b) The Company will take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the third party upon request without delay.

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

(d) The third party will not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for CDD, including done by a third party and undertaking enhanced due diligence measures, as applicable, will rest with the Company.

A. Customer Due Diligence (CDD) Procedure in case of Individuals

For undertaking CDD, the Company will 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:

(a) the Aadhaar number where,

(i) he/she 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

(ii) he/she decides to submit Aadhaar number voluntarily to the Company notified under first proviso to sub-section (1) of section 11A of the PML Act;

or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) 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;

(ac) the KYC Identifier with an explicit consent to download records from CKYCR;

and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c)such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE:

Provided that where the customer has submitted,

(i) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company will carry out offline verification.

(ii) an equivalent e-document of any OVD, the Company will 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 as specified under Digital KYC Process.

(iii) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company will carry out verification through digital KYC as specified under Digital KYC Process.

(iv) KYC Identifier under clause (ac) above, the Company will retrieve the KYC records online from the CKYCR in accordance with RBI guidelines.

Provided that for a period not beyond such date as may be notified by the Government for a class of Regulated Entities, instead of carrying out digital KYC, the Company 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.

In case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme, owing to injury, illness or infirmity on account of old age or otherwise and similar causes, the Company will apart from obtaining the Aadhar 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 will invariably be carried out by an official of the Company and such exception handling will also be a part of the concurrent audit.

The Company will ensure to duly record the cases of exception handling in a centralised exception database. The database will 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 will be subjected to periodic internal audit/inspection by the Company and will be available for supervisory review.

Explanation 1: The Company will, 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.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., will be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

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

(d) Accounts opened using Aadhar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

I. There must be a specific consent from the customer for authentication through OTP.
II. As a risk-mitigating measure for such accounts, the Company will ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar.
III. For borrowal accounts, only term loans will be sanctioned. The aggregate amount of term loans sanctioned will not exceed rupees sixty thousand in a year.
IV. Borrowal accounts, opened using OTP based e-KYC will not be allowed for more than one year unless identification as mentioned above or as mentioned below (V-CIP) is

carried out. If Aadhaar details are used under V-CIP, the process will be followed in its entirety including fresh Aadhaar OTP authentication.

V. If the CDD procedure as mentioned above is not completed within a year for borrowal accounts, no further debits will be allowed.

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

(e) Currently the Company is not opening any retail accounts under Simplified procedure, however, at its own discretion the Company will open retail accounts under simplified procedure, where the balances in all the accounts taken together will not exceed rupees fifty thousand at any point of time as per the prescriptions of RBI's Master direction- Know Your Customer (KYC) direction, 2016.

B . Enhanced Due Diligence

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding:

Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures will be undertaken by the Company for non-face-to-face customer onboarding.

a) V-CIP, will be provided as the first option to the customer for remote onboarding. The processes complying with prescribed standards and procedures for V-CIP will be treated on par with face-to-face CIP

b) In order to prevent frauds, alternate mobile numbers will not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions will be permitted only from the mobile number used for account opening. - mobile number.

c) Apart from obtaining the current address proof, the Company will verify the current address through positive confirmation before allowing operations in the account. Positive confirmation will be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) The Company will obtain PAN from the customer and the PAN will be verified from the verification facility of the issuing authority.

e) First transaction in such accounts will be a credit from existing KYC-complied bank account of the customer.

f) Such customers will be categorized as high-risk customers and accounts opened in non-face to face mode will be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

C. Video based Customer Identification Process (V-CIP) may be undertaken to carry out:

(i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a proprietorship firm, the Company will also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Annexure-I for Sole Proprietorship firm, apart from undertaking CDD of the proprietor.

(ii) Updation/Periodic updation of KYC for the above eligible customers.

While implementing V-CIP, the Company will adhere to the minimum standards on Infrastructure, Procedure and Record Management as detailed in Annexure – II

D. CDD measures for identification of Beneficial Owner (BO):

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) will be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his/her identity will be undertaken keeping in view the following:

a) Where the customer or the owner of the controlling interest is a Company listed on a stock exchange in India, or is a subsidiary of such a Company, or is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place will be obtained.

E. Unique Customer Identification Code (UCIC):

The Company would ensure that it's customers do not have multiple identities within the Company through adequate de-duplication procedures and issuance of a Unique Customer Identification Code (UCIC) for each customer. The UCIC will help the Company to identify customers, track the loan facilities availed, monitor all transactions in a holistic manner and enable the Company to have an effective approach to risk profiling of customers. Further, this

would also help in smoothening the financial transactions for customers. The detailed procedure for issuance of UCIC and dedupe process are managed by the concerned units.

F. Sharing KYC information with Central KYC Records Registry (CKYCR):

In terms of provision of Rule 9(1A) of PML Rules 2005, Company will capture customer's KYC records and upload the KYC data as per the KYC templates (and updated from time to time) prepared for 'Individuals' and 'Legal Entities' (LEs) on to CKYCR within 10 days of commencement of an account based relationship with the customer.

Company will upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR.

Once KYC Identifier is generated by CKYCR, the Company will ensure that the same is communicated to the individual / LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Company will upload / update the KYC data pertaining to accounts of individual customers and LEs at the time of periodic updation, or as and when the updated KYC information is obtained / received from the customer.

Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to Company, with an explicit consent to download records from CKYCR, Company will retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer will not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

i. there is a change in the information of the customer as existing in the records of CKYCR;
ii. the current address of the customer is required to be verified;
iii. the Company considers it necessary to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client
iv. the validity period of documents downloaded from CKYCR has lapsed.

G. Original Seen and Verified (OSV) Norms:

All KYC documents provided by the customer (for applicant/co-applicant /guarantor and other related parties) should be sighted in original and verified by the Employee of the Company/ group Company (as per the agreed terms) and signed with "Original Seen and Verified" with Employee Code under stamp of the Company/ on behalf of the Company.

H. Monitoring of High Risk and Medium Risk Customers:

Due diligence for High risk and Medium Risk customers identification will be as follows:

a) Non-resident customers, due diligence including email verification of employment of the

customer, collection of a local guarantor & power of attorney along with their identification proofs and verification of their residence/office will be done, if found necessary.

b) High net worth individuals, with less than six months occupational track record due diligence including personal discussion with the applicant, analysis of bank statement and financial statements will be done, details of client profile, sources of fund will be obtained, if required.

c) Trusts, charities, NGOs and organizations receiving donations, as and when such cases are received due diligence to be undertaken as for other cases in the high risk categories.

d) Companies having close family shareholding or beneficial ownership, due diligence including personal discussion with the applicant will be done. In case of Company's proportionate income being considered to the extent of the customer's Shareholding in the Company, board resolution authorising the director(s) to sign on behalf of the Company will be collected. Also signature verification of the person(s) issuing the board resolution will be collected, if necessary.

e) Firms with 'sleeping partners', due diligence including personal discussion with the applicant will be done. If income of the partnership firm is being considered, then the Company will collect a letter signed by all the partners authorizing the concerned partner(s) to sign on behalf of the partnership to be continued. Also signature verification of the person(s) issuing this authority letter will be collected, if necessary.

f) 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. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

In addition to the RBI definition of PEP (specified above), the Company chooses to expand the classification of PEPs to include Members of the Parliament (MPs), members of Legislative Assemblies (MLAs), members of Legislative Counsels (MLCs), and prominent figures of major political parties .

Risk Management

The Company has laid down procedures for assessing the risk profiles of its customers and to apply various Anti Money Laundering measures keeping in view the risks involved in transaction, account or business relationship.

For Risk Management, the Company will have a risk - based approach as mentioned in KYC Master

Direction which includes the following:

(a) Customers will be categorised as low, medium and high-risk category, based on the assessment and risk perception.

(b) The Risk categorisation will be undertaken based on parameters such as customer's identity, social/ financial status, nature of business activity and information about the clients' business, their location, type of products/services offered, etc. While considering customer's identity, the Company may confirm identity documents through online or other services offered by issuing authorities.

(c) The risk categorization of a customer and the specific reasons for such categorization will be kept confidential and will not be revealed to the customer to avoid tipping off the customer.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

The Company has a proper Internal Control system in place, which is capable of identifying and evaluating risks and mitigating them by way of reviewing and reporting such risks.

For the new retail products, the risk will be assessed and incorporated in the product note.

The Company has applied a Risk Based Approach (RBA) for mitigation and management of the risks (identified on it's own or through national risk assessment) and has requisite controls, and procedures in place. The Company has implemented a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, the Company monitors the implementation of the controls and enhance them if necessary.The periodicity of risk assessment exercise will be at least annual.

A. Identification of class of customers under various risk categories:

i. **High Risk:** Non-resident customers (track record/vintage less than 180 days), High net worth individuals (track record/vintage less than 180 days), Trusts, charities, NGOs and organizations receiving donations, Companies having close family shareholding or beneficial ownership, Firms with sleeping partners, Politically exposed persons (PEPs), Non-face to face customers, Large Dealers in jewellery, gold/silver/bullions, diamonds and other precious metals/stones (Loan more than INR 10 lacs), those with dubious reputation as per available public information, etc.

Enhanced due diligence measures based on the risk assessment may be applied, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

ii. **Medium Risk**: Self Employed/Proprietors/Partnership firms customers with little known track

record, High net worthindividuals – track record more than 180 days, Business activity relating to Real estate, Hotel industry, Travel Agency, Used car sales, Dot-com Company or internet business, Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, Small Dealers in jewellery, gold/silver/bullions, diamonds and other precious metals/stones (Loan less than INR 10 lacs), etc.

Customers that are likely to pose a higher than average risk may be categorized as medium or highrisk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.

iii. **Low Risk**: customers who are salaried employees, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, People working with Public Sector Units, Resident individuals, Government Departments & Government owned companies, regulators and statutory bodies, Senior Citizens, Pensioners, Self Help Groups, Entities whose identities and sources of fund can be easily identified, People workingwith reputed Public Limited companies & Multinational Companies etc.

Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA), RBI guidelines/instructions and PEL policy.

Not to open an account (except as provided in this Policy) where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed as per the risk categorization, due to non-cooperation of the potential customer or non-reliability of the data/ information furnished to Company. Further, in case of an existing account, where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed as per the risk categorization, due to non-cooperation of the customer or non-reliability of the data/ information furnished to Company, the account will be closed as per extant regulatory prescriptions.

In case of Retail loans, authority for opening/closing of accounts of politically exposed accounts should be exercised by one level above the authorized officer.

For Wholesale loans if any BO, Director, Promoter is a PEP then such details should be highlighted in the Credit Approval Memo for approval of the loan sanctioning authority.

B. Periodic updation of KYC (i.e. Re-KYC):

The Company will 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.

The Company will carry out periodic updation at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC verification or review subject to the following conditions.

a) Individual Customers:

i. **No change in KYC information**: A self-declaration from the customer in this regard will be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, mobile application of the Company, letter etc.

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

iii. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in above (under OTP based e KYC) are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.
Declaration of current address, if the current address is different from the address in Aadhaar, will not require positive confirmation in this case. The Company will 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.

b) Customers other than individuals:

i. **No change in KYC information**: A self-declaration in this regard will be obtained from the Legal Entity (LE) customer through its email id registered with the Company, mobile application of the Company, letter from an official authorized by the LE in this regard, board resolution etc. Further, the Company will ensure during this process that Beneficial Ownership (BO) information available with the Company is accurate and will update the same, if required, to keep it as up-to-date as possible.

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

c) Additional measures:

In addition to the above, the Company will ensure –

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

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

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Post updation of the records in the Company's database an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. Periodic updation of the KYC can be availed at any branch of the Company.

d) The Company will 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 will submit to the Company, the update of such documents. This will be done within 30 days of the update to the documents for the purpose of updating the records at Company's end.

VI. Monitoring of Transactions

On-going monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration that the transactions in the accounts are consistent with the Company's knowledge about the customers, customers' business and the risk profile and risk sensitivity of the account and the source of funds / wealth.

The Company must pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The extent of monitoring will be aligned with the risk category of the customer.

Higher risk accounts will be subjected to intense monitoring. Company will carry out the periodic review of risk categorization of transactions/customer's accounts at a periodicity of not less than 6 months.

- For wholesale portfolio, Company will carry out the periodic review of risk

categorization of transactions/customer's accounts at a periodicity of not less than 6 months and if deemed necessary, apply enhanced due diligence measures on case to case basis.

- For retail portfolio, the Company will carry out Biannual review wherein the name screening of all customers will be conducted. In case there are true sanction or PEP alerts as deemed necessary, an enhanced due diligence measures on case to case basis will be carried out.

The following activities may form part of the monitoring function:

- The account of the Customer after signing of the contract to be closely monitored for signs of any unusual transactions

- All Cash & suspicious transactions are required to be reported within the timelines given under Prevention of Money laundering Act (**'PMLA'**), 2002; the PML Rules 2005 framed thereunder; and the Foreign Regulation Act 2010

- High-risk accounts will be subjected to intensified monitoring.

- The Company should maintain a record of all transactions and take steps to preserve the same.

VII. Record Management

The record management will be in accordance with Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and as advised by RBI from time to time.

Maintenance of records of transactions

The Company has a system of Maintenance of records in its Loan Management System, for each branch/representative office and a consolidated record for all the branches/representative offices taken together at the centralized location, of transactions (nature and value), in such form and for such period as specified under the Rule 3 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

The Company will maintain all necessary information in respect of transactions prescribed under Rule 3 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, so as to permit reconstruction of individual transaction, including the following:

(a) the nature of the transactions;
(b) the amount of the transaction and the currency in which it was denominated;
(c) the date on which the transaction was conducted; and
(d) the parties to the transaction
The Company will 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, the Company will register the details on the DARPAN Portal. The Company will 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

VIII. Reporting Requirements to FINANCIAL INTELLIGENCE UNIT – INDIA (FIU-IND)

a. Appointment of Designated Director

Managing Director/ Chairman of the Company will be appointed as the Designated Director in compliance of Rule 2 (ba) of the Maintenance of Record Rules of the PMLA.

'Designated Director' means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and the Rules thereunder and will be nominated by the Board.

The name, designation and address of the Designated Director will be communicated to the FIU-IND and RBI (along with contact details). In no case, the Principal Officer will be nominated as the 'Designated Director'.

The Designated Director will be responsible to ensure overall compliance specified under the Act and the Rules/ Regulations thereunder.

b. Appointment of Principal Officer (PO)

The Company has appointed the Principal Officer in compliance of Rule 2 (f) of the Maintenance of Record Rules of the PMLA. 'Principal Officer' (PO) means an officer at the management level nominated by the Company responsible for furnishing information as per Rule 8 of the Rules.

Company has designated a senior employee as the PO who will be located at the Head/Corporate office and will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The PO will maintain close liaison with FIU-IND, enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The name, designation and address of the Principal Officer was communicated to the FIU-IND and RBI (along with contact

details).

The Principal Officer will report information relating to cash transactions, suspicious transactions and returns as prescribed by FIU-IND, following the reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility, etc.

If an employee suspects/identifies a Suspicious transaction, it will be reported by that employee through his/her Head of Department (HOD) or directly on the following e-mail ID: Principal.Officer@piramal.com, without any delay.

On receipt of information related to suspicious transaction, the Principal Officer will get the same investigated and after ascertaining that the transaction is indeed suspicious and requires reporting, will report such transaction to the FIU-IND within prescribed timelines.

The Company, its Directors, every employees will maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions and it will be ensured that there is no tipping off to the customer at any level. The Principal Officer under the supervision and guidance of the Designated Director will be responsible to ensure overall compliance specified under the Act and the Rules/ Regulations thereunder. If 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 will not pursue the CDD process, and instead file an STR with FIU-IND.

Indicative List of Suspicious Action & Transactions are set out in Annexure - III

c. Regulatory Reporting to FIU-IND

The Company will maintain the record of all transactions including, the record of:

i. all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

ii. all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;

iii. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions; and

iv. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rule 3(1) (D).

v. The Company will ensure timely and correct reporting is done while furnishing information to the Director, FIU-IND, without delay .The Company will not put any restriction on operations in the accounts merely on the basis of the STR filed.

The Company will maintain proper record of all transaction as prescribed under Rule 3, of the Prevention of Money-Laundering (Maintenance of records of the nature and value of transactions) and RBI Guidelines.

IX. Requirements/obligations under International Agreements

Company Will ensure that no 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) are opened. The details of the two lists are as under:

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

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

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

Details of accounts resembling any of the individuals/entities in the lists will be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566February 2, 2021 (Annex II of the Master Direction - KYC Direction, 2016).

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time will also be taken note of.

X.Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of the Master Direction-KYC Direction, 2016 captioned Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967) will be strictly followed and meticulous compliance with the Order issued by the Government will be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

Further, following to be referred in the Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated from time to time)

Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.(Annex II of the Master Direction - KYC Direction, 2016).

Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005". (Annex III of the Master Direction - KYC Direction, 2016).

XI. Other Related Matters

Selling Third party products

The Company if acting as agent while selling third party products, it will comply with the applicable laws/regulations, including system capabilities for capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers.

Adherence to Know Your Customer (KYC) guidelines and persons authorized by the Company including brokers/agents etc.

a. Persons authorized by the Company for selling loan related products, its brokers/ agents or the like, will be fully compliant with the KYC guidelines applicable to the Company.

b. All information will 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 authorized by the Company including brokers/ agents etc. who are operating on its behalf.

XII. Customer Education/Employee's Training/ Employee Hiring

a) Adequate screening mechanism **including Know Your Employee / Staff policy** as an integral part of Company's personnel recruitment/hiring process has been put in place.

b) The Company would prepare specific education material so as to educate the customers on the objectives of the KYC program.

c) Train the frontline employees of the Company to handle KYC/AML/CFT related matters

d) Put in place an ongoing employee training module so that the staffs are adequately trained on KYC/AML/CFT aspects.

XIII.Compliance of KYC policy

I. The Company will ensure compliance with KYC Policy through:

(a) Senior management as defined below:
- Wholesale Business: As defined in the Delegation of Power Policy
- Retail Business: Chief Operating Officer, National Credit Head, National Head Operation, Compliance Officer

(b) The above defined officials have the responsibility for effective implementation of policies and procedures.

(c) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements will be conducted by an independent audit.

(d) Concurrent/internal audit system will verify the compliance with KYC/ Anti-Money Laundering (AML) policies and procedures.

(e) The Company will submit quarterly audit notes to the Audit Committee.

II. The Company will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

Review of Policy

The Company will review the policy on an annual basis or at earlier intervals, if there any regulatory changes necessitating such interim reviews.

Annexure – I

Customer Identification Procedure-

Certified documents or its equivalent e-documents that will be obtained from the customers at the time of account opening are as below:

Customers	**Documents**
Individuals and individual (Sole Proprietor) Proof of identity and proof of residence	One of the following certified Document or the equivalent e-documents thereof viz., i. Passport ii. Aadhaar Card (mandatory for any subsidy benefit) or Proof of possession of Aadhaar issued by UIDAI or E-Aadhaar. iii. Voter's Identity Card issued by the Election Commission of India iv. Driving License v. Job card issued by NREGA duly signed by an officer of the State Govt. vi. Letter issued by Registrar of National Population Register containing details of name and address And Permanent Account Number (PAN) or Form No. 60 as per Income Tax Rules 1962. (mandatory along with one of the OVDs) 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. A document will 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 Gazette notification or marriage certificate issued by the State Government, indicating such a change of name. In case the OVD furnished by the customer does not contain updated address, the following documents will be deemed to be OVDs for the limited purpose

	of proof of address: (i) Utility bill (electricity, telephone, post-paid mobile phone, piped gas, water bill) not more than 2 months old (ii) Property or municipal tax receipt; (iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (iv) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation; In case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India will be accepted as proof of address Provided further that the customer will submit updated OVD with current address within a period of three months of submitting the above documents.

Sole Proprietorship Firm	Apart from Customer identification procedure as applicable to the proprietor any two of the following certified copy of documents or equivalent e-documents thereof in the name of the proprietary concern would suffice: (i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government (ii) Certificate/ license issued by the municipal authorities under Shop and Establishment Act. (iii) Sales and income tax returns. (iv) CST/VAT/GST certificate (provisional/ final) (v) Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities. (vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax authorities. (viii) Utility bills such as electricity, water, and landline telephone bills In cases where the Company is satisfied that it is not possible to furnish two such documents, it would have the discretion to accept only one of those documents as activity proof. In such cases, the Company, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy that the business activity has been verified from the address of the proprietary concern.

Company	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Certificate of incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the Company; (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; (v) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (vi) the names of the relevant persons holding senior management position; and (vii) the registered office and the principal place of its business, if it is different.
Partnership Firms	One certified copy of each of the following documents or the equivalent e-documents thereof: (i) Registration certificate; (ii) Partnership deed; (iii) Permanent Account Number of the partnership firm; (iv) one copy of an OVD containing details of identity and address, one recent photograph and Permanent Account Number or Form 60 of the beneficial owners, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (v) the names of all the partners; and (vi) address of the registered office, and the principal place of its business, if it is different.

Trusts & Foundations	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Certificate of registration, if registered ii. Trust Deed iii. Permanent Account Number or Form No.60 of the trust iv. Power of Attorney granted to transact business on its behalf v. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors vi. Resolution of the managing body of the foundation/association vii. the names of the beneficiaries, trustees, settlor protector, if any and authors of the trust viii. the address of the registered office of the trust; and ix. list of trustees and documents, as specified for those discharging role as trustee and authorised to transact on behalf of the trust. x. Provided that in case of a trust, the Company ensures that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions

Unincorporated Association or Body of Individuals	One certified copy of each of the following documents or the equivalent e-documents thereof: i. Resolution of the managing body of such association or body of individuals ii. power of attorney granted to him to transact on its behalf iii. PAN or Form 60 of the unincorporated association or body of individuals iv. One copy of an OVD containing details of identify and address, one recent photograph and Permanent Account Number (PAN) or Form 60 of the person holding an attorney to transact on its behalf v. Such other documents as may be required by Company to collectively establish the legal existence of such as association or body of individuals.

*'Officially valid document(OVD)' is defined to mean the passport; the driving license; Voter's Identity Card issued by the Election Commission of India; Letter issued by the Unique Identification Authority of India, containing details of name, address and proof of possession of Aadhaar Number; Job Card issued by NREGA duly signed by an officer of the State Government; Letter issued by the National Population Register containing details of name and address or any other document as notified by the Central Government / RBI. Alternatively, in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), the certified copy 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.

The Company will where its customer submits his Aadhaar number, ensure that such customer redact or blackouts his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

The use of Aadhaar, proof of possession of Aadhaar etc., will be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

Annexure – II

(a) V-CIP Infrastructure

i) The Company should comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction will necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it will be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data will be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

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

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

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

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

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

vii) The V-CIP infrastructure will 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 will be mitigated before rolling out its implementation. Such tests should be conducted bythe empanelled auditors of Indian Computer Emergency Response Team (CERT-In).. Such tests should also be carried out periodically in

conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services will 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 will also be carried out periodically in conformity with internal/ regulatory guidelines.

Note:

The requirement of technical infrastructure being housed in the premises of the Company doesn't mean that it can't use the cloud deployment model. It will be ensured that the ownership of the data in such model rests with the Company only and data including video recording is transferred to the RE's exclusively owned/ leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data will be retained by the cloud service provider or third party technology provider assisting the V-CIP of the Company.

(b) V-CIP Procedure

i) Company will formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process will be operated only by officials of the Company specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) 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 will be initiated.

iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions will be varied in order to establish that the interactions are real-time and not pre-recorded.

iv) Any prompting, observed at end of customer will lead to rejection of the account opening process.

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

vi) The authorised official of the Company performing the V-CIP will record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) Offline Verification of Aadhaar for identification
b) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer.
c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Company will ensure to redact or blackout the Aadhaar number.
In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it will 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.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, The Company will 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, the Company will ensure that no incremental risk is added due to this.

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

viii) The Company will 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 will be verified from the database of the issuing authority including through Digilocker.

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

x) The authorised official of the Company will 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 will match with the details provided by the customer.

xi) All accounts opened through V-CIP will be made operational only after being subject to

concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

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

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP will be stored in a system / systems located in India. The Company will 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.

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

Annexure III

Suspicious Action & Transactions (Indicative only)

- Builder is unable to explain the sources of funding for the project
- Approvals/sanctions from various authorities are proved to be fake
- Customer is reluctant to provide information, data, documents
- Submission of false documents, data, purpose of loan, details of accounts.
- Refuses to furnish details of source of funds/own contribution.
- Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons.
- Transactional activity (level or volume) suddenly changes and/or is inconsistent with the customer's apparent financial standing, their usual pattern of activities or occupational information
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist)
- Transactions involving any countries deemed high risk or non-cooperative by the Financial Action Task Force
- Transactions involve persons or entities identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities
- Applying for a loan knowing fully well that the property/dwelling unit to be financed has been funded earlier and that the same is outstanding
- Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase
- Multiple funding of the same property/dwelling unit
- Request for payment made in favour of a third party who has no relation to the transaction
- Usage of loan amount by the customer in connivance with the vendor/builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated
- Overpayment of instalments with a request to refund the overpaid amount.