CAPITAL INDIA
Home Loans

Policy on Know Your Customer Guidelines and Anti-Money Laundering Measures

Version	:	12.0
Owned By	:	Operations
Approved By	:	Board of Directors
Effective From	:	November 03, 2023

1. Introduction

Reserve Bank of India ("**RBI**") and National Housing Board ("**NHB**") have, from time to time, issued the guidelines on Know Your Customer ("**KYC**") and Anti Money Laundering ("**AML**") Measures for the regulated entities including the housing finance companies for setting the standards for prevention of money laundering activities and corporate practices while dealing with their Customers from time to time.

Capital India Home Loans Limited ("**Company**") has adopted a robust policy framework on KYC and AML measures in line with the guidelines prescribed by RBI and/or NHB ("**Policy**"). The Company shall adopt all the best practices prescribed by RBI and/or NHB from time to time and shall make appropriate modifications to the Policy, if necessary, to conform to the standards so prescribed. The contents of the Policy shall always be read in conjunction with the changes / modifications which shall be advised by RBI and/or NHB from time to time.

2. Objective:

The objective of the Policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers (*defined hereinafter*) and its financial dealings in better way which in turn will help the Company to manage its risks prudently.

3. Applicability:

This Policy shall prevail over anything else contained in any other document, process, circular and / or instruction that has been issued by the Company in this regard and shall be applicable to all verticals and products of the Company, whether existing or rolled out in future.

4. Definitions:

In this Policy, unless there is anything in the subject or context inconsistent therewith, the expressions listed below shall, when capitalized, have the following meanings:

"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (as amended from time to time) ("**Aadhaar Act**").

"Beneficial Owner (BO)" shall mean:

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: (i) "Controlling ownership interest" means ownership of/entitlement to more than 10% (Ten percent) 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 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 off entitlement to more than 10% (Ten percent) of capital or profits of the partnership.

c) Where the Customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership off entitlement to more than 10% (Ten 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.

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% (Ten 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.

"Board" shall mean the board of directors of the Company.

"Cash Transactions" shall mean "Cash Transactions" as defined under rule 3 of the PML Rules.

"Central KYC Records Registry" or "CKYCR" shall mean an entity (i.e. currently, Central Registry of Securitization Asset Reconstruction and Security Interest of India ("CERSAI")) defined under Rule 2(1)(aa) of the PML Rules, to receive, store, safeguard and retrieve the KYC records of a Customer in digital form.

"Certified Copy" - obtaining a certified copy by the Company, shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or Officially Valid Document or any other 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 PMLA.
Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
b) branches of overseas banks with whom Indian banks have relationships,
c) Notary Public abroad,
d) Court Magistrate,
e) Judge,
f) Indian Embassy/Consulate General in the country where the nonresident customer resides.

"Committee" shall mean the Credit Committee or Risk Committee of Board, as may be specified by the Board from time to time.

"Definition of Non-profit organization" entity or organisation constituted for religious or charitable purposes as referred to in Section 2(15) of the Income Tax Act, 1961 and is registered.

Details while establishing/onboarding customers; By way of the amendment, the requirement of additional documents have been stated in Rule 9(6), 9(7) and 9(8), which is to be submitted by the client to the reporting entity.

After Rule 9(9), two sub-rules, namely Rule 9(9A) and Rule 9(9B) are inserted. Rule 9(9A) requires every Banking company or Financial Institution or intermediary to register the details of a client, which is a non-profit organization and not already registered, on the DARPAN Portal of NITI Aayog. The registration record to be maintained for a period of five years of the business relationship between a client and a reporting entity has ended or the account has been closed, whichever is later. Rule 9(B) contemplates that the clients subm its updates of the already submitted documents under Rule 9(4), Rule 9(5), Rule 9(6), Rule 9(7), Rule (8) and Rule 9 (9) with the reporting entity, within 30 days of the updation.

"Customer" shall mean a Person, who is engaged in a financial transaction or activity with the Company and includes a Person on whose behalf the Person who is engaged in the Transaction or activity, is acting.

"Customer Due Diligence" or "CDD" shall mean identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

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

a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

"Customer Identification" means undertaking the process of CDD.

"Designated Director" shall mean a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and shall be nominated by the Board of the Company.

"Digital KYC" shall mean 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 PMLA and PML Rules.

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

"Equivalent E-document" shall mean 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.

"FATCA" shall mean Foreign Account Tax Compliance Act of the United States of America (U.S.) 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.

"**HNI**" shall mean high net worth individuals.

"**KYC Identifier**" means the unique number or code assigned to a Customer by the Central KYC Records Registry

"**KYC Templates**" shall mean templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities, as applicable.

"Non-Face-to-Face Customers" shall mean Customers who open the accounts without visiting the branch/ offices of the Company or meeting the officials of the Company.

"Officially Valid Document" or **"OVD"** shall mean the passport, the driving license, proof of possession of Aadhaar number, voter's identity card issued by election commission of India, job card issued by NREGA duly signed by an officer of the state government, the letter issued by the national population register containing details of name, address or any other document as notified by the central government with the regulator.

Further, where the Customer submits his/her/its proof of possession of Aadhaar number as an officially valid document, he/she/it may submit it in such form as are issued by the Unique Identification Authority of India.

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

"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)

"Periodic Updation" shall mean 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 RBI and/or NHB.

"**Person**" shall have the same meaning as defined in the PMLA 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 and (g) any agency, office or branch owned or controlled by any of the above persons.

"Politically Exposed Persons" (**PEP**) shall mean individuals who are or have been entrusted with prominent public functions e.g., heads of States / Government, senior politicians, senior government / judicial / military officers, senior executives of state owned corporations, important political party officials, etc.

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

"Principal Officer" shall mean an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the PML Rules.

"**PMLA**" shall mean the Prevention of Money Laundering Act, 2002, including all the rules / regulations made pursuant thereto, as amended from time to time.

"**PML Rules**" shall mean Prevention of Money-laundering (Maintenance of Records) Rules, 2005, as amended from time to time.

"Suspicious Transaction" shall mean "Suspicious Transaction" as defined under rule 2(g) of the PML Rules and the amendments thereto.

"Transaction" shall mean "Transaction" as defined under rule 2(h) of the PML Rules and the amendments thereto.

"Video based Customer Identification Process" or **"V-CIP"** shall mean an alternate method of customer identification with facial recognition and customer due diligence by an authorized 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 Policy.

5. Key elements of the Policy:

This Policy includes 4 (Four) key elements, details of which are given below:

- Customer Acceptance Policy ("**CAP**")
- Risk Management
- Customer Identification Procedures ("**CIP**")
- Monitoring of Transactions.

5.1 Customer Acceptance Policy ("CAP"):

(i) CAP lays down the criteria for acceptance of the Customers. The guidelines in respect of the Customer relationship in the Company broadly includes the following:

a) No account shall be opened in anonymous or fictitious / benami name(s).
b) No account shall be opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the Customer or non-reliability of the documents/information furnished by the Customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
c) No Transaction or account-based relationship shall be undertaken without following the CDD procedure.
d) The mandatory information which is required to be obtained from the Customers for KYC purpose while opening an account and during the Periodic Updation, shall be specified.
e) Any optional / additional information if required from the Customers after the account is opened, shall be obtained with the explicit consent of the Customers.

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

g) In case of an existing KYC compliant Customer, there shall be no need for a fresh CDD exercise.

h) Circumstances in which, a Customer is permitted to act on behalf of another person/ entity, shall be clearly spelt out.

i) Suitable system shall 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 circulated by RBI / NHB from time to time.

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

k) A Unique Customer Identification Code shall be allotted while entering into new relationships with individual Customers as also the existing Customers.

l) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002 (Central Act No. 15 of 2003) (hereinafter referred to as PMLA), rules framed thereunder and guidelines issued from time to time

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

n) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.

(ii) The Company shall ensure that the adoption of CAP and its implementation shall not result in denial of services of the Company to general public, especially to those, who are financially or socially disadvantaged.

5.2 Risk Management:

(i) The Company shall put in place an effective KYC program by establishing appropriate procedures and ensuring their effective implementation, which shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. The Company shall allocate the responsibility for ensuring that the policies and procedures of the Companies are implemented effectively.

(ii) The Risk categorization shall be undertaken based on parameters such as Customer's identity, social financial status, nature of business activity, and information about the Customer's business / occupation and their location etc.

(iii) Customers that are likely to pose a higher than average risk to the HFC may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. HFCs may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include

(iv) The Recommendations made by the Financial Action Task Force (FATF) on AML standards and on Combating Financing of Terrorism (CFT) standards shall also be used in risk assessment.

5.3 Customer Identification Procedures ("CIP"):

Rule 9 of the Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), requires every HFC:

at the time of commencement of an account–based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship, and
in all other cases, verify identity while carrying out :
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.

(i) For the purpose of verifying the identity of the Customers at the time of commencement of an account-based relationship, the Company may, in its sole discretion, rely on CDD done by a third party, subject to the following conditions:
   a) Records or the information of the CDD carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
   b) Adequate steps are taken by the Company to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements shall be made available from the third party upon request without delay.
   c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with CDD and record-keeping requirements in line with the requirements and obligations under the Prevention of Money-Laundering Act.
   d) The third party shall 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, shall rest with the Company.

(ii) The Company may, alternatively, undertake Video based Customer Identification Process (V-CIP), as specified under Annexure IV.

5.4 Monitoring of Transactions:

Monitoring of Transactions is an essential element of effective implementation of the Policy, which shall be conducted taking into consideration the risk profile and risk sensitivity of the Customers. The Company shall make an endeavor to understand the normal and reasonable activity of the Customer so that Transactions which fall outside the regular/pattern of activity can be identified. Special attention shall be paid to all complex, unusually large Transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

(i) Maintenance of records of Transaction:

A Company shall maintain the records of Transactions (nature and value), entered into between the Company and the Customer, and records of the identity and address of the Customer, in such form and for such period as specified under the PML Rules and the guidelines issued by

RBI / NHB.

A Company shall maintain all necessary information in respect of Transactions prescribed under Rule 3 of the PML Rules, 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 shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) so that the information can be retrieved easily and quickly whenever required or requested by the competent authorities.

(ii) **Furnishing of information to the Director, Financial Intelligence Unit – India (FIU-IND):**

The Company shall, inter-alia, without any delay, furnish to the Director FIU-IND, within such time and in such form, the information in respect of Transactions as referred under sub-rule (1) of rule 3 of the PML Rules and a copy of such information shall be retained by the Principal Officer for the purposes of official record.

The Company shall not put any restriction on operations on the accounts where a Suspicious Transaction Report has been filed. The Company shall keep the fact of furnishing of Suspicious Transaction Report strictly confidential and shall ensure that there is no tipping off to the Customer at any level.

The Company may put in use a robust software, throwing alerts when the Transactions are inconsistent with risk categorization and updated profile of the Customers, as a part of effective identification and reporting of Suspicious Transactions.

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

The Company shall adhere to the provisions of income tax rules, FATCA and CRS, as applicable and shall take all appropriate steps for complying with the reporting requirements.

The Company shall also adhere to United Nations Security Council Resolutions (UNSCRs) circulated by the RBI, (as applicable) in respect of any other jurisdictions / entities from time to time.

(iv) **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 and amendments thereto, the Company 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).

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND, Ministry of Home Affairs and/or RBI / NHB, as may be required under the applicable laws.

The Company shall strictly follow the procedure laid down in the UAPA order dated February 2, 2021, as may be amended from time to time and shall ensure meticulous compliance with such order issued by the government.

6. Money Laundering and Terrorist Financing Risk Assessment:

The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' as per the procedures and controls specified in the **Annexure VI.**

7. Customer Due Diligence (CDD) Procedure:

7.1. Procedure for obtaining identification and CDD Measures:

The Company shall undertake CDD the procedures and measures described in **Annexure II** hereto in relation to the Customers.

7.2. On-going Due Diligence:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk by understanding the normal and reasonable activities of the Customer.

The Company shall 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 shall be aligned with the risk category of the Customer.

The Company shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk Customers, especially those for whom the sources of funds are not clear. Periodic review-based risk categorization of accounts will be carried out atleast once in 6 (Six) months and would be based on exceptional reporting like google alerts and other market information. In case, no such information is received, existing classification of the Customers shall continue.

7.3. Periodic Updation:

The 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. However, Periodic Updation shall be carried out at least once in every two years for high-risk Customers, once in every eight years for medium risk Customers and once in every ten years for low risk Customers from the date of opening of the account / last KYC updation.

a) Individual Customers:

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

ii) **Change in address:** In case of a change only in the address details of the Customer, a self-declaration of the new address shall be obtained from the Customer through Customer's

email-id registered with the Company, Customer's mobile number registered with the Company, digital channels (such as mobile application of the Company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, a copy of OVD or deemed OVD or the equivalent e-documents thereof, as specified in the Policy, for the purpose of proof of address, declared by the Customer at the time of Periodic Updation may be obtained from the Customer.

iii) Accounts of customers, who were minor at the time of opening account, on their becoming major: In case of Customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Comapny. Wherever required, The Company may carry out fresh KYC of such Customers i.e., Customers for whom account was opened when they were minor, on their becoming a major.

b) Customers other than individuals:

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

ii) Change in KYC information: In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for onboarding a new LE Customer.

c) Additional measures: In addition to the above, the Company shall ensure that,

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

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

iii) Acknowledgment is provided to the Customer mentioning the date of receipt of the relevant document(s), including self-declaration from the Customer, for carrying out Periodic Updation. Further, the information / documents obtained from the Customers at the time of Periodic Updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the Customer.

iv) In order to ensure Customer convenience, the Company may consider making available the facility of Periodic Updation of KYC at any branch / office.

8. Appointment of Designated Director and Principal Officer:

Designated Director:

The name, designation, and address of the Designated Director, including changes from time to time, shall be communicated to the Director, Financial Intelligence Unit India (FIU-IND) and also to RBI and/or NHB, as may be required.

Principal Officer

The Board has nominated Mr. Rachit Malhotra, being Chief Compliance Officer and Company Secretary of the Company, as a 'Principal Officer' who shall be responsible for ensuring compliance, monitoring Transactions, and sharing and reporting information as required under the PMLA and PML Rules. The name, designation, and address of the Principal Officer, including changes from time to time, shall be communicated to the Director, FIU-IND and also to RBI and/or NHB, as may be required.

9. Other Measures:

9.1. Secrecy Obligations and Sharing of Information:

The Company shall maintain secrecy regarding the Customer information which arises out of the contractual relationship between the Company and the Customer. 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 Transactions.

An illustrative (but not exhaustive) list of Suspicious Transactions financial services (including housing / builder / project loans) is furnished under Annexure III.

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

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the PML Rules, as required by the revised KYC Templates prepared for Individuals and Legal Entities ("LE") as the case may be. The Company shall upload the KYC data with CERSAI in respect of all accounts, as required under the provisions of the PML Rules, from time to time.

The Company shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the PML Rules.

The Company shall capture Customer's KYC records and upload onto CKYCR within such period as may be specified under PML Rules and / or guidelines / circulars issued by RBI or NHB, as applicable. Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the Customer.

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

i) there is a change in the information of the Customer as existing in the records of CKYCR;
ii) the current address of the Customer is required to be verified;
iii) the Company considers it necessary in order to verify the identity or address of the Customer, or to perform enhanced due diligence or to build an appropriate risk profile of the Customer.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs (opened prior to April 1, 2021) at the time of Periodic Updation or earlier, when the updated KYC information is obtained/received from the Customer. The Company shall ensure that during Periodic Updation, the Customers are migrated to the current CDD standard.

9.3. Hiring of Employees and Employee training:

The Company shall put in place an adequate screening mechanism as an integral part of the personnel recruitment/hiring process. The Company shall also put in place an on-going employee training programme so that the members of staff are adequately trained in KYC/AML Measures 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.

9.4. Selling Third party products:

The Company, while acting as agents to sell third party products, shall comply with the applicable laws/regulations, including system capabilities for capturing, generating and analyzing alerts for the purpose of filing cash transaction report / suspicious transaction report in respect of Transactions relating to third party products with Customers.

9.5. Adherence to KYC guidelines by the Company and persons authorized by the Company including brokers/agents etc.

All persons authorized by the Company for selling loan related products, their brokers/ agents or the like, shall be fully compliant with the KYC guidelines applicable to the Company.

All information may be made available to RBI / NHB 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 their behalf.

9.6. Closure of Accounts/Termination of Financing/Business Relationship:

In case the Company is unable to apply appropriate CDD procedures or measures due to non-furnishing of information and/or non-cooperation by the Customer, the Company shall consider closing the account or terminate business relationship after issuing due notice to the Customer explaining the reasons for taking such a decision. Such action shall be taken with the approval of Chief Executive Officer of the Company or Head – Risk of the Company or any other Key Managerial Personnel of the Company duly authorized for this purpose.

9.7. Internal Control System and compliance with the Policy:

The Company shall ensure compliance with the Policy through:
(i) concurrent/ internal audit system to verify the compliance with KYC/Anti-Money Laundering (AML) policies and procedures;

(ii) submission of quarterly audit notes and compliance to the Audit Committee.

The Internal Auditors of the Company shall check and evaluate the adherence and compliance of the Policy. A compliance report of the Internal Auditors shall be submitted to the Committee on quarterly basis.

10. Review of the Policy:

This Policy is subject to review by the Board, as and when deemed necessary. The Board may amend or revise this Policy from time to time, as required under the guidelines issued by RBI and/or NHB and other applicable laws.

Notwithstanding anything contained in this Policy, the Company shall ensure compliance with any additional requirements as may be prescribed under the provisions of PMLA, PML Rules, Foreign Contribution and Regulation Act, 1976, and other applicable laws / regulations, either existing or arising out of any amendment to such laws / regulations or otherwise and applicable to the Company from time to time. Any change/amendment in PMLA, PML Rules, Foreign Contribution and Regulation Act, 1976 and other applicable laws shall be deemed to be incorporated in this Policy by reference and this Policy shall be deemed to have been amended and revised accordingly.

11. Record Keeping.

11.1 Maintenance of records and Transactions : The Company shall maintain proper record of the transactions as required under Section 12 of the PML Act read with the Rule 3 of the PML Rules.

The records required to be maintained in the relation to the PML Rules, including transactions mentioned above shall contain the following information:

I. The nature of the transaction;
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.

11.2. Preservation of records: The Company shall maintain, preserve and report records as required in terms section 12 of PML Act and the Master Directors, including as under;

a) All the transactions with the customer, both domestic or international – for a minimum period of 5 (Five) years from the date of transactions.
b) Records of the identity of all the customer and their addresses for the minimum period of 5 (Five) years from the date of cessation of the transaction/ business relationship with the Customer.

The company shall take appropriate steps to evolve a system for proper maintenance and preservation of information (in hard and/or soft copies) in a manner that allows such data to be retrieved easily and quickly whenever required or as and when requested by competent authorities.

The Company shall upload the KYC data pertaining to all new and existing accounts, as required in terms of the Master Directors, with the Central Registry of Securitization Asset Reconstruction and Security Interest India (CERSAI), in accordance with the PML Rules.

The Operations Teams of the company shall be responsible of compliance of the above provisions in relation to Record Keeping and preservation of records.

12. Compliance of this Policy:

1) The Company shall have an ongoing employee training program so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for the frontline staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.
2) The senior management of the Company shall ensure effective implementation of this policy by putting in place appropriate procedures to ensuring their effective implementation, covering proper management oversight, systems and controls, segregation of duties, training and other related matters.
3) The company shall utilize risk-based approach to address management and mitigation of various AML risks and ensure concurrent/internal audit and independent evaluation to verify the compliance with this policy and procedures, including legal and regulatory compliances under the PML Act, PML Rules, the guidelines issued by NHB.

ANNEXURE I - Risk Categorization of the Customers:

This Annexure refers to risk categorization of Customers and is indicative only.

High Risk – Category A	Medium Risk – Category B	Low Risk – Category C
a) Non – Resident Indian (NRI) Customers; b) HNIs-Persons who have applied for loan amount more than 5 crores. c) Self-employed Customers with sound business and profitable track record for less than 3 years d) Trust, charitable organizations, Non-Government Organization (NGO) and organizations receiving donations; e) Companies having close family shareholding or beneficial ownership with group track record of less than 5 years; f) Firms with sleeping partners; g) Politically Exposed Persons (**PEPs**) of Indian/ foreign origin; h) Person with dubious reputation as per public information available; i) Persons without any contact number and details; j) Person with criminal background; k) Persons engaged in the business of real estate, including builders and developers. l) Non Face To Face Customers	a) Salaried applicant with variable income/ unstructured income receiving, salary in cheque; b) Salaried applicant working with private limited companies (excluding those part of any large group companies / MNCs), proprietary, partnership firms; c) Self-employed Customers with sound business and profitable track record for more than 3 years; d) Companies having close family shareholding or beneficial ownership with group track record of more than 5 years.	a) Salaried employees with well-defined fixed salary received through bank credit; b) People working with government owned companies, regulators and statutory bodies, MNCs, rated companies, PSUs, public limited companies, etc. In the event of an existing Customer or the Beneficial Owner of an existing account subsequently becoming a PEP, the Company will obtain the approval of Chief Executive Officer or Head – Risk or any Key Managerial Personnel in such cases to continue the business relationship with such person, and undertake enhanced monitoring, in terms of this Policy.

ANNEXURE II

Part I: CDD Measures:

The Company shall undertake CCD measures while establishing an account- based relationship with the Customers. Following are the details and documents which shall be verified and obtained from the Customers.

Customer	Documents
In case of Individuals:	Each of the following documents: i) One recent photograph; ii) Certified Copy of any of the following OVD or Equivalent e-document thereof, containing details of identity and address, - Passport, - Driving license, - Voter's identity card, - Proof of possession of Aadhaar number*. iii) Permanent account number or Equivalent e-document thereof, or Form No. 60 iv) Such other identity card / document or the Equivalent e-document thereof. (subject to the satisfaction of the Company) In case the OVD furnished by the Customer does not contain updated address, the following documents or Equivalent e-document thereof, shall be deemed to be OVD for the limited purpose of proof of address: i) Utility bill which is not more than 2 (Two) months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii) Property or Municipal tax receipt; iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv) Letter of allotment of accommodation from employer issued by state government or central department, statutory or regulatory bodies, public sector undertaking, structured commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation. Provided that the Customer shall submit updated OVD with current address within a period of 3 (Three) months of submitting the above documents. Provided further that where the Customer has submitted, i) proof of possession of Aadhaar where Offline Verification can be carried out, the Company shall carry out Offline Verification, ii) an Equivalent e-document of any OVD, the Company shall verify the Digital Signature as per the

	provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annexure V**, iii) proof of possession of Aadhaar number where Offline Verification cannot be carried out or any OVD, the Company shall carry out verification through Digital KYC as specified under **Annexure V** or 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, for a period not beyond such date as may be notified by the government from time to time. Further, where a Customer has provided his/her Aadhaar number for identification and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he/she may give a self-declaration to that effect to the Company, as per the guidelines stipulated by RBI / NHB, from time to time. *Note: Wherever Aadhaar number is provided by a Customer as OVD, the Company shall ensure that the Customer redacts or blacks out the Aadhaar Number from the OVD through appropriate means prior to submission of the same. Where Permanent Account Number is obtained, the same shall be verified from the verification facility of the issuing authority However, Aadhaar number is required to be submitted by the Customers who are desirous of availing / receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act (including any interest subsidy under Pradhan Mantri Awas Yojana), at the time of making an application for availing such subsidy.
In case of Sole Proprietary Firms: For Proprietor For the Proprietary Firm	Documents as required to be obtained for individuals. Any two of the following documents or Equivalent e-document thereof,: i) Registration certificate. ii) Certificate / licence issued by the municipal authorities under Shop and Establishment Act. iii) Sales and income tax returns. iv) CST/VAT/CST 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 DCFT/Licence/ 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, the Company may, at its discretion, accept only one of those documents as proof of business/activity. Provided the Company shall undertake a 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.
In case of Companies:	Certified copies of each of the following documents or Equivalent e-document thereof, to be obtained: i) Certificate of incorporation, ii) Memorandum & Articles of Association, iii) Permanent account number of the company, iv) Resolution from the board of directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact business on behalf of the company, v) In respect of managers, officers or employees, as the case may be, holding an attorney to transact on behalf of the company: - one copy of OVD containing details of identity and address, - one recent photograph and - Permanent account number or Form 60.
In case of Partnership Firms:	Certified copies of each of the following documents or Equivalent e-document thereof, to be obtained: i) Registration certificate, ii) Partnership deed, iii) Permanent account number of the partnership firm, iv) Power of attorney granted to a partner or an employee of the firm to transact business on behalf of the partnership firm, v) In respect of the person holding an attorney to transact on behalf of the partnership firm: - one copy of OVD containing details of identity and address, - one recent photograph and - Permanent account number or Form 60.

In case of Trusts:	Certified copies of each of the following documents or Equivalent e-document thereof, to be obtained: i) Registration Certificate, ii) Trust deed, iii) Permanent Account Number or Form No.60 of the trust, iv) Power of attorney granted to any person transact business on behalf of the trust, v) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust. vi) the address of the registered office of the trust; and vii) list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust viii) In respect of the person holding an attorney to transact on behalf of the trust: - one copy of OVD containing details of identity and address, - one recent photograph and - Permanent Account Number or Form 60.
In case of Unincorporated Association or a Body of Individuals:	Certified copies of each of the following documents or Equivalent e-document thereof, to be obtained: i) resolution of the managing body of such association or body of individuals, ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals; iii) power of attorney granted to any person to transact on behalf of such association or body of individuals, iv) In respect of the person holding an attorney to transact on behalf of such association or body of individuals: - One copy of OVD containing details of identity and address, - one recent photograph and - Permanent account number or Form 60, v) such other information as may be required by the Company to collectively establish the legal existence of such as association or body of individuals. Explanation - Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals, includes societies.
In case of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats.	Certified copies of each of the following documents or Equivalent e-document thereof, to be obtained: i) Document showing name of the person authorized to act on behalf of such entity; ii) Permanent account number / OVD for proof of identity and address in respect of the person holding an attorney to transact on behalf such entity; and iii) Such documents as may be required by the Company to establish the legal existence of

	such an entity/juridical person. iv) 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 or when carrying out transactions as specified under Customer Identification Procedure

CDD Measures for Identification of Beneficial Owner

For opening an account of a legal person who is not a natural person (individual), the Beneficial Owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his/her/its identity shall be undertaken keeping in view the following:

(a) Where the Customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or Beneficial Owner of such companies.

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

Part II: Enhanced Due Diligence Measures

Accounts of Non-Face-To-Face Customers:

In the case of Non-Face-To-Face Customers of the Company, apart from applying the usual Customer Identification Procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of cross-border Customers, there is the additional difficulty of matching the Customer with the documentation and the Company may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place. The Company shall ensure that the first payment is to be effected through the Customer's KYC-complied account, for enhanced due diligence of Non-Face To Face Customers

Accounts of Politically Exposed Persons (PEPs):

The Company shall gather sufficient information pertaining to PEPs and check all the information available on the Person in the public domain. The Company shall verify the identity of the Person and seek information about the sources of funds before accepting the PEP as a Customer. The decision to provide financial services to an account for PEP shall be taken at a senior level and such accounts shall be subjected to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs. 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 be applicable to to family members or close associates of PEPsis the Beneficial Owner.

Customer's accounts opened by Professional Intermediaries:

The Company shall, while opening Customer's accounts through professional intermediaries, ensure that:

a) The Customer shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b) The Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

c) The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.
d) All the Beneficial Owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'subaccounts', each of them attributable to a Beneficial Owner, or where such funds are co-mingled at the level of the Company, the Company shall look for the Beneficial Owners.
e) The Company shall, in its sole discretion, rely on the 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.
f) The Company shall hold the ultimate responsibility for knowing the Customer.

ANNEXURE III

Illustrative List of Suspicious Transaction Pertaining to Financial Services:

1) A list of Suspicious Transactions pertaining to Builder / Project / Corporate Clients:

i) Builder approaching the Company for a small loan compared to the total cost of the project;
ii) Builder is unable to explain the sources of funding for the project;
iii) Approvals/sanctions from various authorities are proved to be fake or if it appears that client does not wish to obtain necessary governmental approvals/ filings, etc.;
iv) Management appears to be acting according to instructions of unknown or inappropriate person(s);
v) Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used);
vi) Clients with multijurisdictional operations that do not have adequate centralized corporate oversight;
vii) Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/ corporate seat or other complex group structures);
viii) Entities with a high level of Transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.

2) A list of Suspicious Transactions pertaining to Individual:

i) Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
ii) Unnecessarily complex client structure;
iii) Individual or classes of Transactions that take place outside the established business profile, and expected activities/ Transaction unclear;
iv) Customer is reluctant to provide information, data, documents;
v) Submission of false documents, data, purpose of loan, details of accounts;
vi) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
vii) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
viii) Approaches a branch/ office of a Company, which is away from the Customer's residential or business address provided in the loan application, when there is a branch/ office of the Company nearer to the given address;
ix) Unable to explain or satisfy the numerous transfers in account/ multiple accounts;
x) Initial contribution made through unrelated third party accounts without proper justification;
xi) Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount;
xii) Suggesting dubious means for the sanction of loan;
xiii) Where Transactions do not make economic sense;
xiv) Unusual financial Transactions with unknown source;
xv) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment;
xvi) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
xvii) Encashment of loan amount by opening a fictitious bank account;
xviii) 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;
xix) Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
xx) Multiple funding of the same property/dwelling unit;
xxi) Request for payment made in favour of a third party who has no relation to the Transaction;
xxii) 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;
xxiii) Multiple funding / financing involving NCO / Charitable Organisation / Small / Medium Establishments (SMEs) / Self Help Croups (SHCs) / Micro Finance Croups (MFCs);
xxiv) Frequent requests for change of address;

xxv) Overpayment of instalments with a request to refund the overpaid amount;
xxvi) Investment in real estate at a higher/lower price than expected;
xxvii) Clients incorporated in countries that permit bearer shares.

ANNEXURE IV

Video based Customer Identification Process (V-CIP)

The Company may undertake V-CIP to carry out, (i) CDD in case of new Customer on-boarding for individual Customers, proprietor in case of proprietorship firm, 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 shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, apart from undertaking CDD of the proprietor, (ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication (as applicable), and (iii) Updation / Periodic updation of KYC for eligible Customers.

The Company, while opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure:

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

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

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

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

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

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

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

viii) The V-CIP application software and relevant APIs / webservices 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.

(b) V-CIP Procedure:

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

ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

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

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

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

vi) 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 (as applicable)
- Offline Verification of Aadhaar for identification
- KYC records downloaded from CKYCR, using the KYC identifier provided by the Customer
- Equivalent e-document of OVDs including documents issued through Digilocker.

The Company shall ensure to redact or blackout the Aadhaar number. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 (Three) days from the date of carrying out V-CIP. Further, in line with the prescribed period of 3 (Three) days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within 3 (Three) days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.

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

viii) The Company shall capture a clear image of PAN card to be displayed by the Customer during the process, except in cases where e-PAN is provided by the Customer. The PAN details shall be verified from the database of the issuing authority including through 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 shall ensure that photograph of the Customer in the Aadhaar/OVD and PAN/e-PAN matches with the Customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the Customer.

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

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

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The 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 guidelines on record management, as stipulated in this Policy, shall also be applicable for V-CIP.

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

ANNEXURE V

Digital KYC Process

a) The Company may develop an application for digital KYC process ("Application") which shall be made available at Customer touch points for undertaking KYC of the Customers and the KYC process shall be undertaken only through such authenticated application of the Company.

b) 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 the Company to its authorized officials.

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

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

e) The Application 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.

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

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

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

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

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

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

regarding transaction-id/reference-id number to Customer for future reference.

l) The authorized officer of the Company shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the Customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.

m) On Successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of Customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the Customer.

ANNEXURE VI

Money Laundering and Terrorist Financing Risk Assessment

Background:

The Reserve Bank of India **(RBI)** introduced an amendment to Master Direction – Know Your Customer (KYC) Direction, 2016 requiring regulated entities to carry out money laundering **(ML)** and terrorist financing **(TF)** risk assessment exercises periodically. This requirement shall be applicable with immediate effect and the first assessment shall be carried out by June 30, 2020.

Undertaking ML and TF risk assessment is a very subjective matter with no standard process to be followed for the same. There is no uniformity on procedures of risk assessment, however, the Company has considered guidance principles enumerated by international bodies for carrying out risk assessment exercise.

Global practices for ML/TF risk assessment:

The concept of ML and TF risk assessment arises from the recommendations of Financial Action Task Force **(FATF)**. Based on FATF recommendations, many jurisdictions have prepared and published risk assessment procedures. India is yet to come up with the same. For example, the national risk assessment of money laundering and terrorist financing is the guidance published by the UK government which provides for sector specific guidance for risk assessment. The sector specific guidance is further granulated keeping in view the specific threats to certain parts of the sector.

Risk assessment process:

The Company has domestic operations and its Customers fall into similar categories and/or where the range of products and services are homogenous and hence a simple risk assessment suffices. The Company is primarily into affordable housing finance and non – home loans are also done with an intent of meeting individual consumption or business capital needs. Thus, the Company track the main purpose and end use of funds for the facility through monitoring of various parameters such as direct payment to seller / vendor for which loan is given, disbursement in verified business account, verification with financial statements, certificate from chartered account among others. In addition to the customer identification procedures as per the Policy approved by the Board, the process of ML / TF risk assessment may be divided into following steps:

Step 1: Collection of information:

- The risk assessment shall begin with collecting of information on a wide range of variables including information on the general criminal environment, TF and terrorism threats, TF vulnerabilities of specific sectors and products, and the general anti-money laundering **(AML)** measures in place.

- The information may be collected externally or internally. It can be fetched through the FI being carried out for the borrower through external empaneled agency. They have repository of records and dedup on same along with google database gives a desired outcome. Any negative remark in this report shall be taken into account by credit team while underwriting the loan proposal.

Step 2: Threat identification

- Based on the information collected, jurisdiction and sector specific threats would be identified based on the risks identified on the national level; however, it shall not be limited to the same and shall be commensurate to the size and nature of business.

- Factors to be considered include the level of inherent risk including the nature and complexity of the Company's loan products and services, size, business model, corporate governance arrangements, delivery channels among others. Focus would also be given to the internal controls in place and the functioning of the internal oversight functions.

Step 3: Assessment of ML/TF vulnerabilities:

- This step involves determination of the how the identified threats will impact the entity / borrower with the probability of risks occurring. Based on the assessment, ML/TF risks should be classified as low, medium and high impact risks.

- While assessing the risks, following indicative factors should be considered:
  - ≥ The nature, scale, diversity and complexity of business and target markets;
  - ≥ The number of Customers already identified as high risk;
  - ≥ The jurisdictions the Company is exposed to, either through its own activities or the activities of Customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT controls and listed by RBI or FATF;
  - ≥ The distribution channels, including the extent to which the Company relies on third parties / business associates to conduct Customer Due Diligence (CDD);
  - ≥ The internal audit and regulatory findings

- This information should be supplemented with information obtained from relevant internal and external sources, such as operational/business heads and lists issued by inter-governmental international organisations, national governments and regulators.

Step 4: Analysis of ML/TF threats and vulnerabilities:

Once potential TF threats and vulnerabilities are identified, the next step is to consider how these interact to form risks including assessment of likely consequences.

Step 5: Risk Mitigation:

Post the analysis of threats and vulnerabilities, appropriate mitigant for the ML/TF risks identified shall be put in place. The initial stages of the CDD process helps to assess the ML/TF risk associated with a proposed business relationship, determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.

Risk identification and its mitigation can be broadly classified based on the following:

- **Business-based risk assessment**: Companu's products, services and delivery channels, the geographical location in which the Company operates along with other relevant factors, if any.

  - Products, Services and Delivery Channels

Examples	Mitigant / Steps to consider
High-risk products and services, such as: • electronic funds transfers,./	• Legitimate products and processes can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product or service. Steps to mitigate may involve assessment of the products and services by the type of market

• products offered through the use of intermediaries or agents	that they are directed to or nature of product (e.g. individuals, or corporate, personal loan etc.) as this may have an impact on the risk. • Additionally, it may be checked whether the products or services allow Customers to conduct business or transactions with higher-risk business segments, or could they be used by Customers on behalf of third parties.
Delivery channels, such as: • Non face-to-face transactions • Business Associate / Agent network	There may be a higher inherent risk with regards to delivery channels in non face-to-face transactions, use agents or if Customers can apply for products online. Adherence to strict AML norms and tracking end usage of funds till the desired party for which loan is meant helps mitigate the risk. Also additional comforting factor could be retail nature of product offering which to an extent mitigates possibility of ML / TF.
New Technologies	• Products/services that are based on new technologies may have an impact on overall inherent risks. • E.g.: new payment methods can be used to transmit funds more quickly or anonymously, such as electronic wallets, pre-paid cards, internet payment services, digital currency or mobile payments.

- Geography

Examples	Mitigant / Steps to consider
Border-crossings: • Air (i.e. airports) • Water (i.e. ports, marinas) • Land • Rail	If business is situated near a border-crossing, there may be a higher inherent risk due to the fact that it may be the first point of entry into the financial system. The Company does not have any such operational presence.
Geographical location and demographics: • Large city • Rural area	• Depending on situation, a rural area where Customers are known to the Company could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. • Governments database details of crime by regions may benefit the assessment. The Company has access to several database to verify and criminal proceedings or any other litigation pertaining to the borrower / individuals.
Connection to high-risk countries: • UN Security Council Resolutions • FATF list of High-Risk Countries and Non-Cooperative Jurisdictions	Certain countries should be identified as posing a high risk for ML/TF based on, among other things, their level of corruption, the prevalence of crime in their region, the weaknesses of their money laundering control regime, or being identified by competent authorities like the FATF or through their respective advisories. The Company business operations and nature of product offerings are not having presence outside India hence risk is mitigated.

- Other Relevant Factors (If applicable)

Examples	Mitigant / Steps to consider
• Ministerial Directives • Regulators	Sanctions can impact business by: • prohibiting trade and other economic activity with a foreign market, • restricting financial transactions such as foreign investments or acquisitions, or • leading to the seizure of property situated in India. These restrictions may apply to dealings with entire countries, non-state actors, such as terrorist organizations from a target country. Any ministerial directives must be taken into consideration and any additional measures to be followed as specified by regulator from time to time.

Business model: • Operational structure • Third party and/or service providers	• Consideration of business model, the size of business, the number of branches and employees, is required to determine if risks exist in relation to this element. E.g.: - A business with several branches and thousands of employees will present different risks than a business that has one location and 2 employees. - A business with a high employee turnover. • This highlights the fact that other compliance regime elements such as training are very much intertwined with risk-based approach exercise. Adequate training – mainly an On The Job training to underwriting team is effectively undertaken by the Company for awareness and better implementation of functional roles. • Use of a third party or service provider can be a good business practice, but the business is ultimately responsible for the compliance regime, client identification, record keeping and reporting obligations. Full understanding of how third party/service provider is functioning is required.

- Relationship-based risk assessment: products and services Customers utilize, the geographical locations in which asset is acquired or they do business as well as their activities, transaction patterns among others.

  - Products, Services and Delivery Channels: The examples as elicited above applied, mutatis-mutandis, to Customers as well.
  - Geography

Examples	Mitigant / Steps to consider
Customer's proximity to an office / branch	A Customer that conducts business or transactions away from its home office / branch without reasonable explanation should be noticed.
Customer is a non-resident	Identification of these Customers may prove more difficult since they may not be present in person and as such, should raise the inherent level of risk.
Customer acquiring asset under consideration away from business place / current residence	A Customer who is proposing to buy a house away from the regular business place or current residence without reasonable justification should be noticed.
Customer has offshore business activities or interests.	Is there a legitimate reason for this? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.

  - Pattern of activity

Examples	Mitigant / Steps to consider
Customer is in possession/ control of / acquiring property that is owned/controlled by/on behalf of a terrorist/a terrorist group	This needs to be highlighted to the government authority.
Customer is a Politically Exposed Foreign Person (PEFP)	A PEFP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence that they may hold, a PEFP is vulnerable to ML/TF or other offences such as corruption. As a business, a politically exposed foreign person is a high-risk Customer.
The account activity does not match the Customer profile	Account activity that doesn't match the Customer profile may indicate a higher risk of ML/TF.
Customer's business generates cash for transactions not normally cash intensive	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.

- Focus on CDD procedure:

  - During the CDD process that the identity of a Customer is verified and risk based assessment of the Customer is done. While assessing credit risks, ML/TF risks shall also be assessed.

  - The risk classification of the Customer, as discussed above, should also be done based on the CDD carried out. The CDD procedure, apart from verifying the identity of the Customer, should also go a few steps further to understand the nature of business or activity of the Customer. Measures should be taken to prevent the misuse of legal persons for money laundering or terrorist financing including transaction due diligence to identify source and application of funds, beneficiary of the transaction, purpose etc.

  - Records on transactions and information obtained through the CDD measures shall be maintained. The CDD information and the transaction records should be made available to competent authorities upon appropriate authority. Some examples of enhanced due diligence measures are as follows:
    ≥ carrying out additional searches (e.g., verifiable adverse media searches)
    ≥ commissioning an intelligence report on the Customer or beneficial owner to understand better the risk that the Customer or beneficial owner may be involved in criminal activity
    ≥ verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
    ≥ seeking additional information from the Customer about the purpose and intended nature of the business relationship
    ≥ seeking information about purpose of buying asset under consideration and its relevance in correlation with data provided in loan application form.

  - Other measures
    ≥ Tracking end usage of funds for which loan is intended to be used becomes the starting point of mitigating ML/TF
    ≥ Monitoring through periodical Credit Risk Monitoring Framework (CRMF) exercises (on sample basis) also involves identifying changes to the usage of asset mortgaged, Customer profile (for example, their behavior, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures.
    ≥ Funds / instances or transactions that are suspicious should be reported promptly to the FIU and in the manner specified by the authorities as per the KYC Policy as already approved.

Step 6: Review and update risk assessment:

Once assessed, the impact of the risk shall be recorded and measures to mitigate the same shall be documented. The information that forms basis of the risk assessment process should be timey updated and shall be put up to the risk management committee of the Company, annually, for its assessment / monitoring. The outcome of this exercise shall be made available to competent authorities and self-regulating bodies, as and when required by them. The entire risk assessment procedure should be carried out in case of major change in the information.