

KNOW YOUR CUSTOMER [KYC] & ANTI MONEY LAUNDERING [AML] POLICY

(Applicable from 1st June 2020 and approved by the Board of Directors on 27th June 2020)

Version - III

1. INTRODUCTION

Pursuant to the notification issued by the Reserve Bank of India on **Know Your Customer (KYC) Direction** guidelines vide its **Master Direction DBR.AML.BC.No.81/14.01.001/2015-16** dated **February 25, 2016** and in line with the amendment in the guidelines issued by the Reserve Bank of India vide its Notification No. DOR.NBFC (HFC).CC.No.111/03.10.136/2019-20 dated 19th May, 2020, Roha Housing Finance Private Limited (RHFPL) has adopted "Know Your Customer:" [KYC] & Anti Money Laundering Policy" originally by the Board of Directors of the Company in its Board Meeting & last revised in the Board Meeting held on 27th June, 2020 and this Policy shall have immediate effect to know/understand their customers and their financial dealings better which in turn would help them manage their risks prudently and prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities.

As per RBI guidelines on KYC policy Roha Housing Finance Private Limited [RHFPL] is required to have its KYC policy for its lending / credit operations / financial dealings in line with extant guidelines framed therein. This KYC policy is also framed keeping in mind the same. The policy has the following four key elements:

- (i) Customer Acceptance Policy;
- (ii) Customer Identification Procedures;
- (iii) Monitoring of Transactions; and
- (iv) Risk management

2. OBJECTIVE:

In view of the foregoing, Key objectives of the KYC and AML Policy are as under:

- (a) To establish a regulatorily compliant KYC mechanism to on-board customers;
- (b) To ensure compliance throughout the life-cycle of customers as per the laid down norms
- (c) To prevent the Company's business channels/products/services from being used as a channel for Money Laundering("ML")/ Terrorist Financing("TF");
- (d) To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Company;
- (e) To ensure compliance with the laws and regulations in force from time to time;
- (f) To protect the Company's reputation;
- (g) To lay down KYC-AML compliance norms for the employees of the Company.

3. DEFINITIONS:

Unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

i. **"Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iii. **"Beneficial Owner (BO)"** means:

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 persons, having 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 25 percent of the shares or capital or profits of the company.

(ii) "Control" shall include the right to appoint a 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, having ownership of / entitlement to more than 15 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, having 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.

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 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

iv. **"Certified Copy" of Officially Valid Document (OVD)**- means obtaining and comparing the copy of the proof of possession of Aadhaar Number where offline verification cannot be carried out or OVD so produced by the customer with the original and recording the same on the copy by the authorized officer under his unique number (such as PF No.

or employee number etc.) . The authorized officer will also attest to the duly signed photograph of the customer.

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 anyone of the following, may be obtained:

- authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas Banks with whom the Company have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/ Consulate General in the country where the non-resident customer resides.

v. **“Central KYC Records Registry”** (CKYCR) means an entity defined under Rule 2(1) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vi. **“Customer”** means 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.

vii. **“Customer Due Diligence”** (CDD) means identifying and verifying the customer and the beneficial owner.

viii. **“Customer identification”** means undertaking the process of CDD.

ix. **“Designated Director”** means a person so designated by the Board to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules thereunder and shall include the Managing Director or a whole-time Director (as defined under the Companies Act, 2013) duly authorized by the Board.

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

xi. **“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

xii. **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

xiv. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individual and legal entities.

xv. "Non-face to face customers" means customers who opens accounts without visiting the branch/office of the Company or meeting the officials of the Company.

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

Provided that,

- a) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b) Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-
 - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii. property or Municipal tax receipt;
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions, and listed companies and leave and license agreements with such employers allotting official accommodation;
- c) The customer shall submit OVD with a current address within a period of three months of submitting the documents specified at b) above;
- d) Where the OVD presented by a foreign national does not contain the details of address, in such case, the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xvii "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)

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

xix. **“Person”** includes: a) an individual, b) a Hindu undivided family, c) a company, d) a firm, e) an association of persons or a body of individuals, whether incorporated or not, f) every artificial juridical person, not falling within any one of the above persons (a to e), and g) any agency, office or branch owned or controlled by any of the above persons (a to f).

xx. **“Periodic Updation”** means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relented by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

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

xxii. **“Principal Officer”** means an officer nominated by the Company for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law/ regulations, and responsible for communicating and furnishing information to FIU-IND under PML Rules.

xxiii. **“Suspicious transaction”** means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- (i) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the PML Act, regardless of the value involved; or
- (ii) appears to be made in circumstances of unusual or unjustified complexity; or
- (iii) appears to not have an economic rationale or bonafide purpose; or
- (iv) 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.

xxiv. **“Transaction”** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- a) opening of an account;
- b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- c) entering into any fiduciary relationship;
- d) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- e) establishing or creating a legal person or legal arrangement.

xxv. "UCIC" means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

xxvi. "Video based Customer Identification Process (V-CIP)" means a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose and to ascertain the veracity of the information furnished by the customer. Such a process shall be treated as a face-to-face process for the purpose of this KYC Policy. *(Wherever applicable)*

xxvii. "Walk in Customer" means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.

All other expressions unless defined herein shall have the same meaning as having been assigned to them, under the RBI's Master Circular – Know Your Customer (KYC) Direction, 2016, the Reserve Bank of India Act, 1935, the Banking Regulation Act, 1949, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. CUSTOMER ACCEPTANCE POLICY (CAP)

The Customer Acceptance Policy will ensure the following aspects of customer relationship:

- (i) No account is opened in anonymous or fictitious/benami name(s);
- (ii) Risk in terms of the location of customer and his clients and mode of payments are duly checked;
 - volume of turnover, social and financial status, etc. will form the basis for categorization of customers into low, medium and high risk
 - customers requiring very high level of monitoring, e.g. Politically Exposed Persons will be given due consideration
- (iii) The Company shall not undertake further transactions like additional disbursements, issuance of cheques/ payment orders, additional Top Up loans etc. (except accepting dues, EMIs and inward funds), with the existing customers/ counter party, if proper KYC documents are not in place.
- (iv) The Company shall not open an account where it is unable to apply appropriate customer due diligence (CDD) measures as specified in Chapter VI of the Know Your Customer Directions, 2016 and reiterated in this policy hereafter either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- (v) The Company shall not undertake a transaction or account-based relationship without following the CDD procedure. CDD procedure shall also be followed for all the joint

account holders while opening a joint account.

- (vi) The Company shall obtain Optional/ additional information only with the explicit consent of the customer after undertaking a transaction or establishing an account-based relationship.
- (vii) The Company shall obtain the information/documents as specified in this policy under the heading 'customer due diligence procedures' for KYC purposes while opening an account and during the periodic updation. However, the documents specified in CDD procedure are in addition to and not in substitution of any other document which the Company may require or is required to be obtained under the law for having an account-based relationship with any legal person or entity including a company, partnership firm, trust, society, etc.
- (viii) The PAN, where obtained, shall be verified from the verification facility of the issuing authority.
- (ix) A Unique Customer Identification Code (UCIC) shall be allotted while entering into a new relationship with individual customers.
- (x) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account or desires to avail additional loan facility, there shall be no need for a fresh CDD exercise.
- (xi) The Company shall permit a customer to act on behalf of another person/ entity only in accordance with the law.
- (xii) To ensure that the identity of the customer, directly or indirectly, does not match with any individual terrorist or prohibited/unlawful organizations, whether existing within the country or internationally, or to ensure that the customer or beneficiary is not associated with or affiliated to any illegal or unlawful or terrorist organization as notified from time to time either by RBI, Government of India, State Government or any other national or international body /organizations, the Company shall maintain a list of individuals or entities issued by RBI, United Nations Security Council, UAPA or other regulatory & enforcement agencies. Identity of the customer to ensure non-resemblance will be verified from the said list in all the cases before acceptance.

Subject to the above norms and cautions, it will be ensured that the above norms and safeguards do not result in any kind of harassment or inconvenience to bonafide and genuine customers, especially those who are financially or socially disadvantaged, and they should not feel discouraged while dealing with the Company.

In such exceptional circumstances before rejection of service to customers on the issue of his identity, necessary approval from a level senior to the officer normally taking such decision should be obtained.

The Company will prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy and as per credit & risk policy and operations manual. The customer profile will contain information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by the Company. At the time of credit appraisal of the applicant the details are recorded along with his profile based on meeting with the applicant apart from collection of applicable documents; this is as

per our credit norms which are incorporated in the operation manual and are in practice. However, while preparing customer profile, the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive.

The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes against monetary consideration. The Company will continue to share our client data with Credit Agencies and empanelled FI agencies and such other organizations/entities subject to confidentiality clause, since the purpose of sharing this information is to ensure risk minimization.

5. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information while establishing a relationship. The Company will obtain sufficient information such as Voter ID card, PAN number, Passport etc.as mentioned in **Annexure I** to the policy, necessary to establish, to our satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

It will be ensured that due diligence is observed based on the risk profile of the customer in compliance with the extant guidelines in place and the same will be available for verification. Besides risk perception, the nature of information/ documents required will also depend on the type of customer (individual, corporate etc). For customers that are natural persons, The Company has to obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. The Company collects identity proof, bank account details and property documents and RHFPL has empanelled Field Investigation agencies who independently verify the applicant's occupation, residence and documents as applicable.

(i) The Company shall undertake identification of the customers in the following cases;

(a) 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

(b) in all other cases, verify identity while carrying out :

- i. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- ii. While entering into the transaction:
 - o of selling third party products as an agent;
 - o of selling the Company's own products and services;
 - o for a non-account based customer/ walk-in customer;
- iii. if the value of a single transaction or series of transactions that appear to be connected is more than rupees fifty thousand.

- iv. When it has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

(ii) Reliance on customer due diligence is done by the third party

The Company for the purpose of verifying the identity of customers, while entering into account-based relationship, may rely on customer due diligence done by a third party, subject to the following conditions:

- (a) Such third party has been duly appointed in writing by the Company for that purpose.
- (b) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or the Central KYC Records Registry.
- (c) Copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available without delay to the Company as and when desired.
- (d) The third party is regulated, supervised, or monitored for and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- (e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

An indicative list of the nature and type of documents that may be relied upon for customer identification is given in the **Annexure I**.

6. RISK MANAGEMENT

"Risk Management" in the present context refers to money laundering, terrorist funding risk, credit, and financial risks associated with a particular customer from the Company's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by the customer.

For Risk Management, the Company shall have a risk-based approach.

- a) The Company shall categorize its customers based on the risk perceived by the Company.
- b) The Company shall categorize its customers into low, medium, and high-risk category, based on the assessment, profiling, and money laundering risk.
- c) The parameters such as customer's identity, social/ financial status, nature of the business activity, and information about the clients' business and their location, etc. shall be considered for the risk assessment.

d) The ability to confirm identity documents through online or other services offered by issuing authorities shall also be factored in determining the risk category of the customer.

e) It is to be mentioned here that various other information collected about different categories of customers relating to the perceived risk, is non-intrusive and in accordance with this Policy.

RHFPL has a procedure for creating Risk Profiles of their new customers based on risk categorization basis the above. Further, the Company shall seek information from its customers which is relevant for the loan and is in conformity with the guidelines. However, the Company may use FATF Public Statement, the reports and guidance notes issued by Government, RBI, or other authorities on KYC/AML procedures in risk assessment. The customers profile with the Company shall remain a confidential document and the information shall not be divulged for cross selling or any other purpose.

RHFPL shall categorize the risk profiles of individual customers into 3 (three) basic categories. The categories along with the illustrative examples are as below:

(i) Low Risk

Low Risk individuals are those individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and the transactions in whose accounts by and large conform to known profile. Low – risk customers shall include

- i. Salaried applicants with salary paid by cheque.
- ii. People working with government departments, government owned companies, regulators and statutory bodies, PSUs etc.
- iii. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
- iv. People working with reputed Public Limited companies & Multinational Companies.

For the purpose of risk categorization the cases where RHFPL internal credit score ≥ 50 shall be categorized as low risk.

(ii) Medium Risk

The medium risk customers shall be categorized on the basis of the customer's background, nature and location of activity, country of origin, sources of funds and client profile. Medium Risk customers shall include;

- i. Salaried applicants with variable income/unstructured income receiving salary via cheque
- ii. Salaried applicants receiving salary via cash
- iii. Salaried applicants working with Private limited companies.
- iv. Self Employed professionals other than HNIs
- v. Self Employed customers with sound business and profitable track record for a reasonable period

For the purpose of risk categorization the cases where RHFPL internal credit score

>= 30 and <=50 shall be categorized as medium risk.

(iii) High Risk

The high-risk customers shall be categorized on the basis of the customer's background, nature and location of activity, country of origin, sources of funds and client profile. High risk customer shall typically include:

- i. non-resident customers
- ii. high net-worth individuals
- iii. trusts, charities, NGOs and organizations receiving donations,
- iv. companies having close family shareholding or beneficial ownership,
- v. firms with sleeping partners
- vi. politically exposed persons (PEPs) of foreign origin
- vii. non face to face to customers and
- viii. Persons with dubious reputation as per public information available.
- ix. Persons whose sources of income are not clear.

The Company shall subject accounts of such customers to intensive due diligence. In the event of an existing customer subsequently becoming a PEP, the Company shall obtain necessary approval of the Senior Management to continue the business relationship with such person and if in the affirmative than the Company will undertake enhanced monitoring at regular intervals.

For effective risk management, the Company shall ensure that it has an effective KYC program. The overall KYC program will cover proper management oversight, systems and controls, segregation of duties, training, and other related matters. Responsibilities will be explicitly allocated within the Company to ensure that the Company's policies and procedures are implemented effectively.

Money Laundering and Terrorist Financing Risk Assessment by the Company

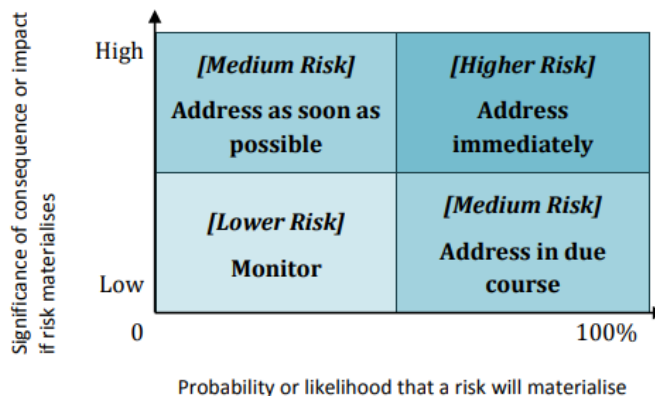
The money laundering and terrorist financing risk for the Company are likely to be low due to the following reasons:

- a) The Company does not operate in other countries /geographies;
- b) The Company does not source/originate loans from other countries/geographies, and its customer base consists of Indian nationals only;
- c) The Company extends loans to identified borrowers for which rigorous KYC checks have been put in place.
- d) The Company verifies the end use of the loan
- e) The Company does not offer banking, liabilities and insurance products; and
- f) The Company offers loans/credit facilities with defined end-use.

However, in accordance with the regulatory requirements, the Company will carry out money laundering and terrorist financing exercise periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk to which the Company may be exposed to. Such internal risk assessment shall be commensurate to its size, geographical presence, the complexity of activities/structure, etc.

The exercise undertaken by the Company shall be properly documented, and the assessment process will consider various relevant risk factors and will take cognizance of overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share. Accordingly, it will frame its mitigation plan also. It should involve the relevant functions and have the following stages:

- a) **Identification:** Development of a list of potential risk factors drawn from known/suspected threats or vulnerabilities. For this purpose, various important aspects of the KYC Policy (non-compliance of which may pose a threat to Company) will be identified along with the risks which the Company may be exposed to due to the same.
- b) **Analysis-** Implementation of key requirements under the KYC Policy should be analyzed. This stage should analyse the likelihood and the impact of each of the identified risks. It will help in assigning priority/ importance to each of the risks.
- c) **Evaluation-** It should involve taking the results found during the analysis process to determine priorities for addressing the risks. These priorities should contribute to the development of a strategy for their mitigation. A typical Risk Evaluation matrix would be as under:



The Company shall conduct the money laundering and terrorist financing Risk Assessment at least once in a year or at such other intervals as may be decided by the Board.

The outcome of the ML and TF Risk Assessment will be put up to the Audit Committee or such other Committee as may be decided by the Board.

7. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

CDD Measures in case of Individuals

While undertaking CDD, RHFPL shall obtain the following information from an individual while establishing an account based relationship with an 'individual' or dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

- 1) Recent photograph;
- 2) Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof;
- 3) Certified copy of one of the OVDs as defined above to be taken for verification of the identity and the address OR the equivalent e-document thereof; and
- 4) Other documents including in respect of the nature of the business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company.

Note:

- (i) If PAN is not available then Form No. 60 as defined in Income-tax Rules, 1962 may be taken;
- (ii) Aadhaar Offline Verification- The Company, being a non-bank, may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purposes. However, where its customer submits his Aadhaar number, the Company will ensure such a customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar Act.
- (iii) Authentication using e-KYC authentication facility provided by the UIDAI- As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the PMLA/ the Aadhaar Act/ the KYC & AML Guidelines.
- (iv) If the customer provides an equivalent e-document of any OVD, the Company should verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules made thereunder and take a live photo as specified under Digital KYC Process defined below
- (v) The Company may also carry-out KYC verification under Digital KYC Process defined below

Video based Customer Identification Process ("V-CIP")

The Company may undertake live V-CIP, to be carried out by an official of the Company, for the establishment of an account-based relationship with an individual customer, after obtaining his informed consent.

The Company, if implements V-CIP, will adhere to the following requirements:

1. The official of the Company performing the V-CIP should record video as well as capture photographs of the customer present for identification and carry out the Offline Verification of Aadhaar for identification.
2. It should capture a clear image of the 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 should be verified from the database of the issuing authority.
3. The live location of the customer (Geotagging) should be captured to ensure that customer is physically present in India.
4. The official should check that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP, and the identification details in Aadhaar/PAN match with the details provided by the customer.

5. The sequence and/or type of questions during video interactions should be varied in order to establish that the interactions are real-time and not pre-recorded.
6. In case of offline verification of Aadhaar using an XML file or Aadhaar Secure QR Code, it should be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.
7. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process.
8. It will be ensured that the process is seamless, real-time, secured, and end-to-end encrypted audio-visual interaction with the customer, and the quality of the communication is adequate to allow identification of the customer beyond doubt. The Company will carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.
9. To ensure security, robustness, and end to end encryption, the Company will carry out software and security audit and validation of the V-CIP application before rolling it out.
10. The audio-visual interaction should be triggered from the domain of the Company itself. The V-CIP process should be operated by officials specifically trained for this purpose. The activity log, along with the credentials of the official performing the V-CIP should be preserved.
11. The Company should ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.
12. The Company will endeavor to take the assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer.
13. The Company should ensure to redact or blackout the Aadhaar number.

Digital KYC Process

In case Digital KYC Process is adopted by the Company, it will ensure compliance with the following requirements:

1. It will use an Application to be made available at customer touch points for undertaking KYC of their customers, and the KYC process shall be undertaken only through this authenticated Application of the Company.
2. The access to such Applications should be controlled by the authorized persons of the Company. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism defined by the Company.
3. The customer, for the purpose of KYC, shall visit the location of the Authorized Official of the Company ("Authorized Official") vice-versa. The original OVD should be in possession of the customer.
4. It should be ensured that the Live photograph of the customer is taken by the Authorized Official, and the same photograph is embedded in the Customer Application Form (CAF). Further, a water-mark in readable form having CAF number, GPS coordinates, Authorized Official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and timestamp (HH:MM:SS) should be put on the captured live photograph of the customer.
5. The Application should have the feature that only a 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 photographs should be of

- white colour, and no other person shall come into the frame while capturing the live photograph of the customer.
6. 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 should be there while capturing the live photograph of the original documents.
 7. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
 8. Thereafter, all the entries in the CAF should 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.
 9. 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 the customer's own mobile number. Upon successful validation of the OTP, it will be treated as a customer signature on CAF. However, if the customer does not have his/her own mobile number, then the 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 the Authorized Official should not be used for customer signature. The Company will check that the mobile number used in the customer signature shall not be the mobile number of the Authorized Official.
 10. The Authorized Official should provide a declaration about the capturing of the live photograph of the 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 official mobile number. Upon successful OTP validation, it shall be treated as the Authorized Official's signature on the declaration. The live photograph of the Authorized Official shall also be captured in this authorized officer's declaration.
 11. Subsequent to all these activities, the Application should give information about the completion of the process and submission of activation request to the activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The Authorized Official shall intimate the details regarding transaction-id/reference-id number to the customer for future reference.
 12. The Authorized Official should check and verify that: (i) information available in the picture of the document is matching with the information entered by the Authorized Official 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.
 13. On Successful verification, the CAF shall be digitally signed by the Authorized Official, who will take a print of CAF, get signatures/thumb-impression of customers at an appropriate place, then scan and upload the same in the system. Original hard copy may be returned to the customer.

Simplified procedure for opening accounts of Individuals

In case a person who desires to open an account is not able to produce any of the OVDs, the Company may at its discretion open accounts subject to the following conditions:

- a) The Company shall obtain a self-attested photograph from the customer.
- b) The authorized officer of the Company should certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
- c) The account shall remain operational initially for a period of 12 months, within which CDD, as prescribed above, should be carried out.
- d) Balances in all their accounts taken together shall not exceed Rs.50,000/- at any point in time.
- e) The total credit in all the accounts taken together shall not exceed Rs.1,00,000/- in a year.
- f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case of Directions (d) and (e) above are breached by him.
- g) When the balance reaches Rs.40,000/- or the total credit in a year reaches Rs.80,000/-, the customer shall be notified that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

For establishing an account based relationship, the authorized official to ascertain as to whether the customer already has a Customer ID with the Company. In case the customer has an existing Customer ID, the new account shall be opened with the same existing Customer ID.

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

CDD Measures for Sole Proprietorship firms:

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

In addition to the above, any two of the following documents or the equivalent e-document thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

- (i) Registration certificate
- (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, the Company may, at its discretion, accept only one of those documents as proof of business activity.

Provided the Company undertakes 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.

CDD Measures for Legal Entities:

Partnership Firm: For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

- (a) Registration certificate
- (b) Partnership deed
- (c) Permanent Account Number of the partnership firm
- (d) Documents, as specified in paragraph 7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

Company: For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

- (a) Certificate of incorporation
- (b) Memorandum and Articles of Association
- (c) Permanent Account Number of the company
- (d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
- (e) Documents, as specified in paragraph 7 above, relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

Trust: For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

- (a) Registration certificate
- (b) Trust deed
- (c) Permanent Account Number or Form No. 60 of the trust

- (d) Documents, as specified in paragraph 7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

Unincorporated Bodies or associations: For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

- (a) Resolution of the managing body of such association or body of individuals;
- (b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals;
- (c) Power of attorney granted to transact on its behalf;
- (d) Documents, as specified in paragraph 7 relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; and
- (e) Such additional information as may be required by the Company, to collectively establish the legal existence of such an association or body of individuals

Explanation:

- i. Unregistered partnership firms/ trusts shall be included under the term 'Unincorporated associations.'*
- ii. Term body of individuals includes 'societies'*

For opening an account of Hindu Undivided Family, certified copies of each of the following documents shall be obtained:

- (a) Identification information, as mentioned under paragraph 7 in respect of the Karta and Major Coparceners,
- (b) Declaration of HUF and its Karta,
- (c) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
- (d) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

Juridical Person: For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

- (a) Document showing name of the person authorized to act on behalf of the entity;
- (b) Documents, as specified in paragraph 7 above, of the person holding an attorney to transact on its behalf; and
- (c) Such other documents as may be specified by the Company in writing to establish the legal existence of such an entity/ juridical person.

Identification of Beneficial Owner

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

- (a) Where the customer or the owner of the controlling interest is 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

8. MONITORING OF TRANSACTIONS & ON-GOING DUE DILIGENCE

- a. Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. The Company will put in place a process to identify and review complex and unusual transactions/ patterns which have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash or are inconsistent with the normal and expected activity of the customer.
- b. The Extent of monitoring shall be aligned with the risk category of the customer, and high risk customer will be subjected to more intensified monitoring.
- c. Since the Company is a housing finance company and all our loans are tenure based with a fixed/variable installment paid through NACH OR any other approved method our monitoring structure will be relevant to our nature of operations. The Company will pay special attention to all unusually large transactions involving large cash and the Company will monitor cash transaction above Rupees Ten lakhs or such other maximum limit prescribed by authorities.
- d. Risk categorization as is mentioned in this policy may be updated as and when required by the management. In case of overdue/default accounts where there is scope for meeting or vetting the profile of this customer gain, due diligence if found necessary will be carried out. Subsequent to our sanction, during the period of part disbursement till full disbursement if any unusual transaction/development comes to our knowledge relating to money laundering the same will be verified and notified as required, The Company will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. The Company will ensure that transactions of suspicious nature as defined in Annexure II and/or any other type of transaction notified under section 12 of the PML Act, 2002, is reported to the appropriate law enforcement authority, as and when detected by our officials through the Principal Officer.
- e. The Company will maintain proper record in accordance with the PML Act, 2002, of all cash transactions (deposits and withdrawals) of Rupees Ten Lakh and above. As a matter of policy, the Company does not accept deposits in cash over Rupees Ten Lakh, No loan is disbursed in cash and No monthly installment above Rupees Ten Lakh is accepted in cash. Any transactions of suspicious nature as per Annexure II are to be reported to the Principal Officer immediately. In addition thereto, the Branches shall on quarterly basis furnish a certificate/mail confirmation to the Principal Officer

evidencing that neither such prohibited transactions and/nor cash transaction as specified in the policy have taken place.

9. PERIODIC UPDATION

Periodic KYC 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 as per the following procedure:

a) RHFPL shall carry out:

- PAN verification from the verification facility available with the issuing authority and
- Authentication, of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.
- In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
- Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorized as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, as self-certification to that effect shall be obtained.
- In case of Legal entities, RHFPL shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- RHFPL may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD / Consent forwarded by the customer through mail/ post, etc., shall be acceptable.
- RHFPL shall ensure to provide acknowledgment with date of having performed KYC updation.
- The time limits prescribed above would apply from the date of opening of the account last verification of KYC.

10. ENHANCED DUE DILIGENCE PROCEDURE

Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given below:

a) **Accounts of non-face-to face customers:**

In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, The Company will do telephonic/personal discussion with the applicant, if necessary. Applicant will be met by the Sales representative of the Company and will fill up the meeting sheet on that basis to mitigate the higher risk involved, as applicable. Certification or Self-attestation where valid of all the documents presented may be insisted upon and, if necessary, additional documents may be called for and applicable verification of these documents will be done. The Company will ensure the first payment is done through any of the KYC Compliant account through banking channels.

b) Accounts of companies and firms

The Company will be careful while processing the cases of business entities specially to establish that individuals are not using those entities for maintaining accounts with it. The Company shall seek information, if required, on the control structure of the entity, source of funds and the natural persons who carry a controlling interest in the management. These requirements may be moderated as per our credit risk policy and guidelines of the operations manual, for e.g. in the case of a public company it will not be necessary to identify all the shareholders.

c) Client accounts opened by professional intermediaries

When the Company has knowledge or reason to believe that the client account opened by a professional intermediary like Direct Selling Agent or Direct selling team or any other sales intermediary by whatever name called is on behalf of a single client, that client will be identified. Where the Company relies on the 'customer due diligence' (CDD) done by an intermediary like Field investigation agency or technical agency or lawyer or any other operation processing intermediary by whatever name called, the Company will ensure that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. The ultimate responsibility for knowing the customer lies with the RE.

d) Accounts of Politically Exposed Persons (PEPs)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions, e.g. Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

The Company will gather sufficient information as available on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. The Company will verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Following aspects shall be considered for PEPs:

- Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- The identity of the person shall have been verified before accepting the PEP as a customer;
- The decision to open an account for a PEP is taken at a senior level in accordance with the RHFPL's Customer Acceptance Policy;
- All such accounts are subjected to enhanced monitoring on an on-going basis;
- all such accounts will be classified as High Risk and will be subjected to required due diligence and monitoring, as applicable
- 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;
- The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner

e) Simplified norms for Self Help Groups (SHGs)

- CDD of all the members of SHG shall not be required while opening the account of SHG.
- CDD all the office bearers of SHG shall suffice.
- No separate CDD under paragraph 7 of the members or office bearers is necessary at the time of extending credit to SHGs.

11. INFORMATION TO BE PRESERVED:

RHFPL shall maintain proper record of transactions as required under section 12 of the PMLA read with Rule 3 of the PML Rules as mentioned below:

- The Company sanctions and disburses files on the system; hence it has a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required. However the Company will maintain account information for at least ten years from the date of cessation of transaction between the company and the client, all necessary records of transactions, both domestic or international, which will make available individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.
- The Company will ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. Apart from this, the application form, copy of loan agreement, NOC, other document either photocopy or cancelled original copy will be kept for next ten years after the full closure of the account. However, preservation and maintenance of the documents will be in paper form or a soft copy.
- The identification of records and transaction data will be made available to the competent authorities upon request only through the principal officer under this policy with his approval.
- introduce a system of maintaining a proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005)
- all cash transactions of the value of more than Rupees Ten lacs or its equivalent in foreign currency.
- all series of cash transactions integrally connected to each other which have been valued below Rupees Ten lacs 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 lacs;

- 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
- all suspicious transactions whether or not made in cash and by way of as mentioned in the Rule 3(1) (D) as mentioned in **Annexure II herein**.
- records pertaining to the identification of the customer and his/her address; and
- should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

The Company will maintain the following information in respect of transactions referred to in the preceding point on "Maintenance of records of transactions"

- i. The nature of the transactions
- ii. The amount of transactions and currency in which it was denominated
- iii. The date on which the transaction was conducted and
- iv. Parties to the transactions

The company shall ensure that their branches continue to maintain proper record of all cash transactions (deposits and withdrawals) of Rs. 10 lakh and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to controlling/head office immediately as and when occurred.

The internal monitoring system shall have an inbuilt procedure for reporting of such cash transactions and those of suspicious nature whether made in cash or otherwise, to the Principal Officer on a fortnightly basis. However, there is no need to furnish NIL reports.

12. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA:

As per Section 12 of PMLA requires every housing finance company to report information of transaction referred to in clause (a) of sub-section (1) of section 12 read with Rule 3 of the PML Rules relating to cash and suspicious transactions etc. to the Director, Financial Intelligence Unit-India (FIU-IND). The proviso to the said section also provides that where the principal officer of a Company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

- i. Cash Transaction Report (CTR)- If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

- ii. Counterfeit Currency Report (CCR)- All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month. Additionally, the Company will submit 'Statement showing the details of Counterfeit Banknotes detected' to the NHB within 7 days from the last day of the respective quarter. Even in the case of 'Nil' instance also, the statement is to be submitted to the NHB
- iii. Suspicious Transactions Reporting (STR)- The Company will monitor transactions to identify potentially suspicious activity. Such triggers will be investigated, and any suspicious activity will be reported to FIU-IND. The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at the conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

The Principal officer will report information relating to cash and suspicious transactions, if detected & reported, in the prescribed formats as designed and circulated by RBI at the following address or through the web site of FIU-IND as per the notification:

The Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri New Delhi-110021

A copy of information furnished shall be retained by the Principal Officer for the purposes of official record.

- A. The information in respect of the transactions referred to in clause(A), (B) and (BA) of sub-rule (1) of rule 3 of the PML Rules (i.e. clauses (i) , (ii) and (iii) referred to in Paragraph 19 supra) is to be submitted to the Director within prescribed time.
- B. The information in respect of the transactions referred to in clause(C) of sub-rule (1) of rule 3 of the PML Rules (i.e. clause(iv) in Paragraph 19 supra) is to be furnished to the Director in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.
- C. The information in respect of the transactions referred to in clause(D) of sub-rule (1) of rule 3 of the PML Rules (i.e. clause(v) in Paragraph 19 supra) is to be furnished promptly to the Director in writing, or by fax or by electronic mail not later than seven working days on being satisfied that transaction is suspicious.
Provided the housing finance company and its employees maintain strict confidentiality of the fact of furnishing/reporting details of suspicious transactions.
- D. It has been advised by the FIU-IND, New Delhi that Company need not submit 'NIL' reports in case there are no Cash/Suspicious Transactions, during a particular

period.

- E. The formats for reporting the requisite information in respect of cash transactions and suspicious transactions are enclosed (Annexures 3 to 10). An illustrative (but not exhaustive) list of suspicious transactions in housing/builder/project loans is furnished in Annexure II.
- F. The required information is to be furnished by the Company directly to the FIU-IND, through the Principal Officer designated by the housing finance company under the Prevention of Money Laundering Act, 2002.

13. MISCELLANEOUS

Compliance under Foreign Contribution (Regulation) Act, 1976 The Company shall also ensure that provisions of the Foreign Contribution (Regulation) Act (FCRA), 1976 are duly adhered to. FCRA regulate the acceptance and utilization of foreign contribution or foreign hospitality received by certain specified persons or associations such as candidates for election, journalist, Judges/Government servants, political party, etc. However, law permits certain persons or associations to accept the foreign contribution with the approval of the Central Government, as per the provisions of FCRA. In those cases, copy of approval or letter of intimation shall be taken from the customer.

RHFPL shall ensure that the provisions of the PML Act, Rules framed thereunder and the Foreign Contribution (Regulation) Act, 2010, applicable, is adhered to strictly.

Sharing KYC information with Central KYC Records Registry (CKYCR)

RHFPL shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015. RHFPL are required to upload the Know Your Customer (KYC) data with CERSAI in respect of new individual accounts opened on or after November 01, 2016

Secrecy Obligations and Sharing of Information

RHFPL shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer. While considering the requests for data/information from Government and other agencies, RHFPL 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. The exceptions to the said rule shall be as under:

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

RHFPL shall maintain confidentiality of information as provided in Section 45NB of RBI Act

1934.

RHFPL shall not use the information collected from the customer for the purpose of cross selling or for any other purpose without the express permission of the customer.

An illustrative (but not exhaustive) list of suspicious transactions in housing/builder/project loans is furnished in Annexure - II.

Reporting Requirement Under Foreign Account Tax Compliance Act (FATCA) And Common Reporting Standards (CRS)

The Company, if applicable, will adhere to the provisions of Income Tax Rules 114F, 114G, and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take requisite steps for complying with the reporting requirements in this regard.

Compliance with Section 51A of Unlawful Activities (Prevention) Act, 1967

The Company will ensure compliance with Section 51A of UAPA Act, 1987 by screening the prospective and existing account holders for UN Sanction List or any other list as per UAPA Act, 1987. In the event, any account holder resembles the name of as per the list, it will be reported to FIU-IND and Ministry of Home Affairs. Further, other requirements including the freezing of assets, shall be followed by the Company.

Adherence to The KYC And AML Guidelines by RHFPL's Agents

- a) The Company's agents or persons authorized by it, for its business, will be required to be compliant with the applicable KYC & AML Guidelines.
- b) All requisite information shall be made available to the RBI/ National Housing Bank to verify the compliance with the applicable KYC & AML Guidelines.
- c) The books of accounts of persons authorized by the Company, including agents, etc., so far as they relate to the business of the company, shall be made available for audit and inspection whenever required.

Selling Third Party Products

The Company acting as agents while selling third party products as per regulations in force from time to time shall comply with the following:

- a. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand
- b. transaction details of the sale of third-party products and related records shall be maintained as prescribed.
- c. Anti-money Laundering (AML) software capable of capturing, generating, and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
- d) transactions involving rupees fifty thousand and above shall be undertaken only by:
 - i. debit to customers' account or against cheques; and
 - ii. obtaining and verifying the PAN given by the account based as well as walk-in customers.

Quoting of PAN

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

Customer Education

The Company will educate the customer on the objectives of the KYC program so that the customer understands and appreciates the motive and purpose of collecting such information.

Hiring of Employees and Employee Training

The Company shall have an ongoing employee training program so that the members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML Measures policies of the Company, regulation and related issues shall be ensured.

No Outsourcing of Decision-making function

The Company shall not outsource decision-making functions of determining compliance with KYC norms

14. Designated Director, Principal Officer, and Senior Management, Internal audit

i. Designated Director:

The Board has designated the Managing Director as the Designated Director to ensure overall compliance with the obligations imposed under this Policy in the matter of KYC compliance or imposed under Chapter IV of the PML Act and the Rules. The Designated Director, in consultation with the Principal Officer, shall be responsible for setting up the policies for implementation of the KYC program and shall issue subsidiary policies or documents for operationalizing the policy. The Designated Director shall allocate responsibilities of officials/departments for ensuring compliance with the KYC Policy.

ii. Appointment of Principal Officer:

The Company has designated DVP- Operations, as 'Principal Officer.' Principal Officer is located at our Corporate Office and will be responsible for monitoring and reporting of all transactions and reporting of information as required under the law. He will maintain close liaison with enforcement agencies, Company and any other institution which are involved in the fight against money laundering and combating financing of terrorism. He will also ensure that there is proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines. However, any such action has to be documented and placed before the management committee of the company. Principal Officer will also report any unusual matter/information to the management committee of the company as and when it

occurs.

iii. **Internal Audit:**

The Company's internal audit department will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. Internal Auditors may specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Audit Committee of the Board along with their normal reporting frequency. A compliance conformation from Branch will be obtained by the Principal Officer.

iv. **KYC for the Existing/new Accounts:**

The Company will apply the KYC norms to the existing customers of loan accounts on the basis of materiality and risk envisaged by it for those existing loan accounts. For deposits the guideline is already in place as advised by NHB, vide their circular NHB (ND)/DRS/Pol-No.02/2004-05 dated August 25, 2004 & as amended from time to time. The Company will ensure that term/recurring deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and are subject to revised KYC procedures.

v. **Non-Cooperation by the customer in respect of KYC norms:**

Where The Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, The Company will follow up with the existing identified customers for KYC compliance, Closure decision if at all is required will depend upon our internal assessment and it will be taken at a Senior Manager at Regional Office/HO, after issuing due notice to the customer explaining the reasons for taking such a decision.

vi. **Applicability to branches and subsidiaries outside India**

The above guidelines will also apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit as and when the Company opens overseas branches. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of National Housing Bank.

Annexure I

Customer identification procedure features to be verified and documents that may be obtained From Customers:

Features	Documents (As per Master Policy updated from time to time)
<p>Individuals Legal name and any other names used</p>	<ul style="list-style-type: none"> • Aadhaar UID / E-KYC verification • Pan Card • Form 60 • Voter's Identity Card, • Driving License (v)Identity Card issued by Govt. authority/ Municipal Corporation / recognized govt. official /public authority (subject to the Company's satisfaction, • Valid Passport • Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Company • Notarized affidavit with photograph duly attested can be accepted for applicant / co-applicant whose income is not considered. • Any one of the other standard ID proof for individual/applicants as per the Credit Policy approved by the Board.
<p>Correct permanent address</p>	<ul style="list-style-type: none"> • Telephone bill • Bank Account Statement • Letter from any recognized public authority • Electricity bill • Ration Card • Letter from employer (Subject to the satisfaction of the Company). • Aadhaar UID / E-KYC verification • Copy of registered Agreement / Sale Deed • Bank Account Statement of Nationalized/Scheduled Commercial Bank.(any one document which provides customer information to the satisfaction of the Company will suffice). • Attested can be accepted for applicant / co-applicant whose income is not considered.

<p>Sole Proprietary Firms</p>	<ul style="list-style-type: none"> ➤ Identification information as mentioned under head 'Individual' above shall be obtained in respect of the individual (proprietor). ➤ In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained <ul style="list-style-type: none"> • Registration certificate. • Certificate/license issued by the municipal authorities under Shop and Establishment Act. • Sales and income tax returns. • CST/VAT/CST certificate (provisional/ final). • Certificate/registration document issued by Sales Tax/Service Tax/ Professional Tax authorities. • IEC (Importer Exporter Code) issued to the proprietary concern by the office of DCFT/ License/ certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • 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. • Utility bills such as electricity, water, and landline telephone bills <p>In cases where RHFPL is satisfied that it is not possible to furnish two such documents, It may, at its own discretion, accept only one of those documents as proof of business/activity. Provided RHFPL undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern</p>
--------------------------------------	--

Legal Entities	
<p>Company</p> <ul style="list-style-type: none"> • Name of the company • Principal place of business • Mailing address of the company • Telephone/Fax Number 	<p>➤ One Certified copy of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> • Certificate of Incorporation • Memorandum & Articles of Association. • Permanent Account Number of the Company • Certificate of Commencement of Business (in case of Public Limited Company) • Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account and/or Power of Attorney granted to its managers, officers or employees to transact business on its behalf • One copy of an OVD containing details of identity and address, one recent photograph and PAN or Form no. 60 of the managers, officers or employees, as the case may be, holding an attorney to transact business on its behalf • Copy of the telephone bill
<p>*Partnership Firms</p> <ul style="list-style-type: none"> • Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners 	<p>➤ One Certified copy of each of the following documents shall be obtained:</p> <ul style="list-style-type: none"> • Registration certificate; • Partnership deed; • PAN of the Partnership Firm; • One copy of an OVD containing details of identity and address, one recent photograph and PAN or Form no. 60 of the managers, officers or employees, as the case may be, holding an attorney to transact business on its behalf; <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> • Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf; • Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses; • Telephone bill in the name of firm/partners;

**Explanation - Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' and the term 'body of individuals, includes societies.*

Annexure II

All suspicious transactions whether or not made in cash and by way of

A. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO HOUSING LOANS:

- 1) Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- 2) Unnecessarily complex client structure.
- 3) Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear
- 4) Customer is reluctant to provide information, data, documents;
- 5) Submission of false documents, data, purpose of loan, details of accounts;
- 6) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc;
- 7) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
- 8) Approaches a branch/office of a RHFPL, which is away from the customer's residential or business address provided in the loan application, when there is RHFPL's branch/office nearer to the given address;
- 9) Unable to explain or satisfy the numerous transfers in the statement of account/multiple accounts;
- 10) Initial contribution made through unrelated third party accounts without proper justification;
- 11) Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
- 12) Suggesting dubious means for the sanction of loan;
- 13) Where transactions do not make economic sense;
- 14) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
- 15) Encashment of loan amount by opening a fictitious bank account;
- 16) 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;
- 17) Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
- 18) Multiple funding of the same property/dwelling unit;
- 19) Request for payment made in favour of a third party who has no relation to the transaction;
- 20) 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.
- 21) Multiple funding / financing involving NGO / Charitable Organisation / Small/Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs)
- 22) Frequent requests for change of address;
- 23) Overpayment of installments with a request to refund the overpaid amount

- 24) Unusual financial transactions with unknown source.
- 25) 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.
- 26) Investment in real estate at a higher/lower price than expected.
- 27) Clients incorporated in countries that permit bearer shares

B. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER/PROJECT LOANS:

- 1) Builder approaching RHFPL for a small loan compared to the total cost of the project;
- 2) Builder is unable to explain the sources of funding for the project;
- 3) 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.;
- 4) Management appears to be acting according to instructions of unknown or inappropriate person(s).
- 5) 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).
- 6) Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.
- 7) 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).
- 8) Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
