

HOMESHREE HOUSING FINANCE LIMITED

KNOW YOUR CUSTOMER (KYC) GUIDELINES AND ANTI-MONEY LAUNDERING (AML) MEASURES

Following the RBI **Master Direction – Non-Banking Financial Company – Housing Finance Company**
(Reserve Bank) Directions, 2021



**HOMESHREE HOUSING FINANCE LIMITED
KNOW YOUR CUSTOMER (KYC)
GUIDELINES AND ANTI-MONEY
LAUNDERING (AML) MEASURES**

Summary of Policy

Policy Name	Know Your Customer (KYC) Guidelines and Anti-Money Laundering (AML) Measures
Date of last review	March 01, 2024
Date of current review	March 31, 2025
Version No.	04
Periodicity of review	Annual
Owner / Contact	Compliance Department
Approver	Board of Directors
Annexures	5

INDEX

Sr. No.	Particulars	Pg No.
1	Preamble & Introduction	4
2	Applicability	4
3	Definitions	4
4	General	9
5	Money Laundering and Terrorist Financing Risk Assessment by HHFL	9
6	Designated Director	9
7	Principal Officer	10
8	Compliance of KYC policy	10
9	Customer Acceptance Policy	11
10	Customer Identification Procedure (CIP)	13
11	Customer Due Diligence (CDD) Procedure	14
12	CDD Measures for Sole Proprietary firms	18
13	CDD Measures for Legal Entities	19
14	Identification of Beneficial Owner	20
15	On-going Due Diligence	20
16	Enhanced and Simplified Due Diligence Procedure	21
17	Accounts of Politically Exposed Persons (PEPs)	22
18	Client accounts opened by professional intermediaries	22
19	Updation / Periodic Updation of KYC	23
20	Risk Management	24
21	Record Management	26
22	Monitoring of Transactions	25
23	Reporting requirements to financial intelligence unit -India	27
24	Requirements/obligations under international agreements communications from international agencies –	29
25	Other Measures	30
26	CDD Procedure and Sharing KYC information with Central KYC Records Registry (CKYCR)	30
27	Hiring of Employees and Employee training:	31
28	Selling Third party products	32
29	Annex-1 Digital KYC Process	33
30	Annex -II Customer identification procedure features to be verified and documents that may be obtained from customers	35
31	Annex -III Suspicious transactions pertaining to housing loans (illustrative list)	40
32	Annex -IV Suspicious transactions pertaining to builder/ project loans (illustrative list)	41
33	Annex -V Red Flags / Parameters To Identify STR	42

CHAPTER-I PRELIMINARY

1. Preamble & Introduction

The objective of 'Know Your Customer (**KYC**) Guidelines' & Anti Money Laundering (**AML**) Measures is to prevent Housing Finance Companies (HFCs) from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable HFCs to know/ understand their customers and their financial dealings better which in turn help them manage their risks prudently.

HomeShree Housing Finance Limited ("**the Company**" or "**HHFL**" or "**RE**") has adopted "Know Your Customer (**KYC**)" and "Anti Money Laundering (**AML**) Measure" (referred to as "**Guidelines**") for lending/ credit/ operations/ financial dealings in line with and as per Master Direction – Know Your Customer (KYC) Direction, 2016 and legal framework on Anti Money laundering (AML) and Countering Financing of Terrorism (CFT) Measures / Obligation of the Company under Prevention of Money Laundering Act (PMLA), 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time.

These Guidelines are framed as per Master Direction – Know Your Customer (KYC) Direction, 2016, updated as on 06th November, 2024, made applicable to Housing Finance Companies vide notification no. **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16** dated November 06, 2024 ("**Master Directions**") and keeping in mind the above and has the following key elements:

- i. Customer Acceptance Policy.
- ii. Customer Identification Procedures.
- iii. Monitoring of Transactions.
- iv. Risk management.

2. Applicability

The provisions of these Guidelines shall apply to the HomeShree Housing Finance Limited (hereinafter referred as '**HHFL**' or '**the Company**' or '**RE**') and to all its Branches / Office except where specifically mentioned otherwise.

These Guidelines are issued under the guidelines issued by National Housing Bank and Reserve Bank of India from time to time and any contravention of or non-compliance with the same may attract penal consequences under the said guidelines.

3. Definitions:

The expressions unless defined herein shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, 1935, Prevention of Money Laundering Act, 2002 (PML Act), Prevention of Money Laundering (Maintenance of Records) Rules, 2005, Master Direction – Know Your Customer (KYC) Direction, 2016, 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.

- 3.1. "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
- 3.2. "**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).
- 3.3. "**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.

3.4. “Beneficial Owner”

Sr. No	Applicable For	Guidelines	
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, has / have a controlling ownership interest or who exercise control through other means.	1) “Controlling ownership interest” means ownership of / entitlement to more than 10 per cent of the shares or capital or profits of the company. 2) “Control” shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
b)	Where the customer is a partnership firm.	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person has/have ownership of / entitlement to more than 10% (Ten percent) of capital or profits of the partnership or who exercises control through other means.	1) “control” shall include the right to control the management or policy decision.
c)	Where the customer is an unincorporated association or body of individuals.	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/ entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.	1) Term ‘body of individuals’ includes “societies” . Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
d)	Where the customer is a trust.	The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.	

3.5. **“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 so produced by the customer with the original and recording the same

on the copy by the authorized officer of the Company as per the provisions contained in the Act.

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:

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

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

3.7. **“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.

3.8. **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

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

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

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

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

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

3.10. **“Designated Director”** means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter-IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors of the Company.

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

- 3.12. **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000.
- 3.13. **"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.
- 3.14. **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S taxpayers hold a substantial ownership interest
- 3.15. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- 3.13 **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- 3.14 **"Non-face-to-face customers"** means customers who open accounts without visiting the branch/ offices of the Company or meeting the officials of the Company.
- 3.15 **"Officially Valid Document"** (OVD) means documents as provided in **Annexure-II** to this policy.
- 3.16 **"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
- 3.17 **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that those are consistent with the company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
- 3.18 **"Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank of India/National Housing Bank.
- 3.18. **"Person"** has the same meaning assigned in the Act and includes:
- a. an individual,
 - b. a Hindu Undivided Family,
 - c. a Company,
 - d. a firm,
 - e. an association of persons or a body of individuals, whether incorporated or not,
 - f. every artificial juridical person, not falling within any one of the above persons (a to e), and
 - g. any agency, office or branch owned or controlled by any of the above persons (a to f).
- 3.19. **"Principal Officer"** means an officer nominated by the Company responsible for furnishing information as per rule 8 of the Rules.
- 3.20 **"Politically Exposed Persons"** (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
- 3.21. **"Suspicious transaction"** means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b) appears to be made in circumstances of unusual or unjustified complexity; or
- c) appears to not have economic rationale or bona-fide purpose; or
- d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

3.22 **“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. the use of a safety deposit box or any other form of safe deposit;
- d. entering into any fiduciary relationship;
- e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- f. establishing or creating a legal person or legal arrangement.

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

3.24. **“Walk-in Customer”** means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.

CHAPTER-II GENERAL

4. The KYC policy shall include following four key elements:
 - (a) Customer Acceptance Policy;
 - (b) Risk Management;
 - (c) Customer Identification Procedures (CIP); and
 - (d) Monitoring of Transactions
5. The “Know Your Customer (**KYC**)” policy is duly approved by the Board of Directors.
6. Money Laundering and Terrorist Financing Risk Assessment by the Company:
 - (a) The Company shall carry out ‘Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment’ exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
 - (b) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
 - (c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.
7. **Designated Director**
 - (a) The Company shall appoint **Managing Director** as the “**Designated Director**” (*nominated by the Board*) to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
 - (b) The name, designation and address of the Designated Director shall be communicated to the FIU- IND.
 - (c) The name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
 - (d) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

8. Principal Officer

The Company shall nominate a senior officer who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

The name, designation and address of the Principal Officer, including changes from time to time shall be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

The name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

9. Compliance of KYC Policy:

(a) The Company shall ensure the compliance of KYC Policy through:

- (i) Senior Management Team for the purpose of KYC Compliance, where “Senior Management Team” comprises of the Managing Director, Chief Risk Officer, Chief Credit Officer/Credit Officer, Chief Compliance Officer, Operations Head, Sales Head, Business Heads and such other officials that the Managing Director may determine from time to time depending upon their functional roles and responsibilities.
- (ii) The Managing Director of the Company is authorized to determine and allocate responsibility for effective implementation of KYC AML policies and procedures at various levels by way of delegation or defining through issuance of office orders or by way of issue of Authority Letters.
- (iii) Independent evaluation of the compliance functions of Company’s policies and procedures, including legal and regulatory requirements to be done by the Managing Director, Chief Risk Officer, Chief Credit Officer/Credit Officer, the Company Secretary and the Chief Compliance Officer of the Company.
- (iv) Internal Audit System to verify the compliance to KYC/AML policies and procedures and submission of quarterly audit notes and compliance to the Audit Committee.
- (v) The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER-III

10. Customer Acceptance Policy

The Company shall frame a Customer Acceptance Policy (CAP). The Customer Acceptance Policy (CAP) is developed laying down explicit criteria for acceptance of customers. The CAP shall ensure that explicit guidelines are in place on the following aspects of customer relationship in the Company.

The Customer Acceptance Policy will ensure the flowing as of customer relationship:

- (i) The Company shall not open an account in anonymous or fictitious/ benami name(s).
- (ii) No account is opened where the Company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer to ensure verification of the identity. 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. However, the Company shall build-in safeguards to avoid any harassment to the customers.
 - i. Permanent Address proof from new customer will be collected. The documents which can be accepted as proof of address as prescribed by NHB/RBI, are mentioned in **Annexure-II**.
 - ii. For customers who wish to pre-close their account with, following will be collected:
 - (a) Permanent Address proof (As per Annexure-II).
 - (b) A declaration from the customer regarding source of funds being used for pre closure of the loan account.
- (iii) No transaction or account-based relationship is undertaken without following the CDD procedure.
- (iv) The Company shall define and categorize the customer into low, medium and high-risk perception on the basis of the location of customer, business profile, his clients, mode of payments, volume of turnover, social and financial status, etc. Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) will be given due consideration and may, if considered necessary be categorized even higher.
- (v) The Company shall collect required documents and other information in respect of different categories of customers depending on perceived low/ medium/ high risk and guidelines issued from time to time. Declaration shall be obtained from the customer that proceedings/ transactions are not in violation of Prevention of Money Laundering (PML) Act 2002 and NHB regulation issued from time to time.
 - a. In the following circumstances, the account may be opened/ operated by a mandate holder or by an intermediary, such as chartered accountants, solicitors, mutual funds, stock brokers etc., in a fiduciary capacity hence the customer is permitted to act on behalf of another person/entity, in conformity with the established law and practices:
 - i. if applicant is NRI/PIO
 - ii. if applicant is a limited company
 - iii. if applicant is a partnership firm

The Company shall ensure, before processing any loan disbursement either by the Company and/or through any specialized agency that the identity of the customer does not match with any person with known criminal background/ with forbidden entities such as individual terrorists or

terrorist organizations, etc. or whose name appears in the sanctions lists circulated by Reserve Bank of India.

- (vi) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- (vii) Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
- (viii) Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
- (ix) CDD Procedure is followed for all the joint account holders, while opening a joint account.
- (x) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
- (xi) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the Master Direction.
- (xii) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- (xiii) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- (xiv) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- (xv) The Company shall prepare a customer profile for each new customer during the credit appraisal process based on risk categorization as mentioned in these guidelines. 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. During the credit appraisal process of the customer, details shall be recorded along with his/ her profile based on meeting with the customer (by the Company representative) apart from collection of applicable documents; this will be as per the Company's credit and product norms which are incorporated in the Credit risk policy and are in practice.
- (xvi) The customer profile will be accorded the status of a highly confidential document and details contained therein shall not be disclosed for cross selling or for any other purposes; unless for the purpose of risk minimization or fraud prevention or required by law & regulations or for social/ economic responsibility.

Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

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

CHAPTER-IV

11. Customer Identification Procedure

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information.

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

- a. At the time of commencement of an account-based relationship, verify the identity of the customer and obtain information on the purpose and intended nature of the business relationship, and
- b. in all other cases, verify identity at the time of processing:
 - i. the transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or multiple transactions that appear to be connected, or
 - ii. any international money transfers operations.
- c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- d. Selling Third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees Fifty Thousand.
- e. When Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- f. The Company shall ensure that introduction is not to be sought while opening accounts.

The Company shall obtain sufficient and reliable documents or information necessary to establish to its satisfaction, the identity of each new customer, (whether regular or occasional) and the clear purpose of the intended nature of relationship. According to the said Rules, the documents/ information to be obtained for identifying various types of customers i.e. individuals, companies, partnership firms, trusts, unincorporated association or a body of individuals and juridical persons.

Customer identification requirements keeping in view the provisions of the said rules are indicated in Annexure-I, also indicative list of the nature and type of documents/ information that may be relied upon for customer identification is given in the Annexure-II. The Company will ensure compliance to the above rule.

The Company shall frame internal guidelines based on their experience of dealing with such persons/entities, normal prudence and the legal requirements.

The Company shall implement the Client Identification Programme to determine the true and correct identity of its customer keeping the above in view.

For the purpose of verifying the identity of customers at the time of commencement of an account- based relationship, Company, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

- (a) Records or the information of the customer due diligence carried out by the third party is obtained within two days 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 customer due diligence requirements shall be made available from the third party upon request without delay.

- (c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- (d) The third party shall not be based in a country or jurisdiction assessed as high risk.
- (e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

CHAPTER-V

12. Customer Due Diligence (CDD) Procedure:

PART-1:

Procedure in case of Individuals

12.1 Procedure in case of individuals:

The Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

- (a) the Aadhaar number where,
 - (i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - (ii) he decides to submit his Aadhaar number voluntarily to the Company as per first proviso to sub-section (1) of Section 11A of the PML Act; or
 - (aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
 - (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
 - (ac) the KYC Identifier with an explicit consent to download records from CKYCR by obtaining OTP; and
 - (b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
 - (c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company.

Provided that where the customer has submitted:

- i) Aadhaar number under clause (a) above to the Company the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Company.
- ii) Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.

- iii) 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-I (Digital KYC Process) of the said directions.
- iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under Annexure-I (Digital KYC Process) of the said directions.
- v) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with paragraph 56 of Master Direction.

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

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

Explanation 1: The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso(i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

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

- i. There must be a specific consent from the customer for authentication through OTP.
- ii. As a risk-mitigating measure for such accounts, the company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. The Company shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.

- iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per paragraph 16 or as per paragraph 18 (V-CIP) of Master Direction is carried out. If Aadhaar details are used under paragraph 18 of the Master Direction, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- viii. declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Company. Further, while uploading KYC information to CKYCR, the Company shall clearly indicate that such accounts are opened using OTP based e-KYC and the Company shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- ix. The Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

12.1.2 The Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations and para 18 of Master Direction:

- 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, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in paragraph 28 and paragraph 29 of Master Direction, apart from undertaking CDD of the proprietor.

- ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per paragraph 17 of Master Direction.
- iii. Updation/ Periodic updation of KYC for eligible customers.
- iv. The official of the Company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:
 - The Company to carry out Offline Verification of Aadhaar for identification.
 - a) 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.
 - b) Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

- v. The official of the Company shall ensure 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 shall match with the details provided by the customer.
- vi. The authorised official of the RE performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
- a) OTP based Aadhaar e-KYC authentication;
 - b) Offline Verification of Aadhaar for identification;
 - c) KYC records downloaded from CKYCR, in accordance with paragraph 56, using the KYC identifier provided by the customer;
 - d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker;
- 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 official of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.
- ix. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.
- x. Further, in line with the prescribed period of three working 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 three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, REs shall ensure that no incremental risk is added due to this.
- xi. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.
- xii. The Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. The Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.
- xiii. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.
- xiv. The audiovisual interaction shall be triggered from the domain of the Company itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

- xv. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.
- xvi. The Company are encouraged to take 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. However, the responsibility of customer identification shall rest with the Company.
- xvii. The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.
- xviii. The activity log along with the credentials of the official performing the V-CIP shall be preserved.
- xix. The Company shall ensure to redact or blackout the Aadhaar number in terms of paragraph 16 of Master Direction.

PART-2:
CDD Measures for Sole Proprietary firms

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

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

- (a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
- (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
- (c) Sales and income tax returns.
- (d) CST/VAT/ GST certificate (provisional/final).
- (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
- (f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
- (h) Utility bills such as electricity, water, landline telephone bills, etc.

12.2.1 In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at their discretion, accept only one of those documents as proof of business/activity.

Provided the Company undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

PART-3:
CDD Measures for Legal Entities

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 16 of Master Direction, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
- (f) the names of the relevant persons holding senior management position; and
- (g) the registered office and the principal place of its business, if it is different.

12.3.1 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 Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- (e) the names of all the partners and
- (f) address of the registered office, and the principal place of its business, if it is different.

12.3.2 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 16 of Master Direction, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- (e) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
- (f) the address of the registered office of the trust; and
- (g) list of trustees and documents, as specified in paragraph 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

12.3.3 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 16 of Master Direction relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
- (e) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'

Explanation: Term 'body of individuals' includes societies.

12.3.4 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 there of shall be obtained:

- (a) Document showing name of the person authorised to act on behalf of the entity;
- (b) Documents, as specified in Paragraph 16 of the Master Direction, of the person holding an attorney to transact on its behalf and
- (c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Provided that in case of a trust, the Company shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of paragraph 13 of the Master Direction.

PART-4: **CDD Measures for Identification of Beneficial Owner**

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

- (a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- (b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

PART-5:
On-going Due Diligence

- 14.** The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds/wealth.

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

- (a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- (b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
- (c) High account turnover inconsistent with the size of the balance maintained.
- (d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

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

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

- (a) *A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.*
- (b) *The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.*

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

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

PART-6:
Enhanced and Simplified Due Diligence Procedure:

15. A. Enhanced Due Diligence

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

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

16. Accounts of Politically Exposed Persons (PEPs):

- A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:
 - (a) The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
 - (b) Reasonable measures are taken by the REs for establishing the source of funds / wealth;
 - (c) the approval to open an account for a PEP shall be obtained from the senior management;
 - (d) all such accounts are subjected to enhanced monitoring on an on-going basis;
 - (e) 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;
- B. These instructions shall also be applicable to family members or close associates of PEPs.

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

17. Customer's accounts opened by Professional Intermediaries:

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

- (a) 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 'sub-accounts', 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, at their 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 ultimate responsibility for knowing the customer lies with the Company.

18. Updation / Periodic Updation of KYC

Periodical updating of KYC shall be taken up or 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) The Company shall carry out:
 - (i) PAN verification from the verification facility available with the issuing authority; and
 - (ii) Authentication, of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.
 - (iii) In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
 - (iv) 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, a self-certification to that effect shall be obtained.
 - (v) In case of Legal entities, the Company shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- b) The Company 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 bonafides. Normally, OVD / Consent forwarded by the customer through mail/ post, etc., shall be acceptable.
- c) The Company shall ensure to provide acknowledgment with date of having performed KYC updation.
- d) The time limits prescribed above would apply from the date of opening of the account / last verification of KYC.

Policy in this regard shall be documented as part of the Company's internal KYC policy duly approved by the Board of Directors of the Company or any committee of the Board to which power has been delegated.

CHAPTER-VI
RISK MANAGEMENT

- 19.** The Management under the supervision of the Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship. Broad principles may be laid down by the REs for risk-categorisation of customers.

The following elements of the Company would manage the Risk arising out of the noncompliance to PMLA:

- (a) As per KYC policy, for acceptance and identification, customers are categorized broadly into low risk, medium risk, and high risk parameters for risk categorization of customers is as under: -
- (A) Low risk customers will be individuals (excluding high Net Worth) and entities whose identities and sources of wealth can be easily identified, have structured income and transactions in whose accounts by and large conform to the known profile. In these cases, only the basic requirements of verifying the identity and location of the customer have to be met. Illustrative examples of low risk customers are asunder:
- i. Salaried employees with well-defined salary structures;
 - ii. People belonging to government departments, regulators, statutory bodies;
 - iii. People working with government owned companies, regulators and statutory bodies etc.
 - iv. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
 - v. People working with Public Sector Units;
- (B) Customers that are likely to pose a higher than average risk to the Company 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. 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. Examples of high risk customers requiring higher due diligence may include:
- Non-resident customers;
 - High net worth individuals, without an occupational track record of more than 3 years;
 - Trusts, charities, NGOs and organizations receiving donations;
 - Companies having close family shareholding or beneficial ownership;
 - Firms with 'sleeping partners';
 - Politically exposed persons (PEPs) of foreign origin;
 - Non-face to face customers;
 - Those with dubious reputation as per available public information, etc.

Politically Exposed Persons (PEPs) will be given due consideration and may, if considered necessary be categorized even higher risk, and their account will be open only after formal approval of senior management, Managing Director. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the Company shall obtain senior management approval in such cases to continue the business relationship, and also undertake enhanced monitoring.

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

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

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc., may also be used in risk assessment.

The Company should examine the background and purpose of transactions with persons from jurisdictions included in the Financial Action Task Force (FATF) Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined and written findings together with all the documents should be retained and made available to the Reserve Bank/ other relevant authorities, on request. The Recommendations made by the Financial Action Task Force (FATF) on Anti-money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards would also be used in risk assessment.

CHAPTER-VII

MONITORING OF TRANSACTIONS

- 20.** Ongoing monitoring is an essential element for effective KYC procedures. However, the extent of monitoring will depend on the risk categorization of the account.

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 Company may prescribe various methods for calculating the threshold limits for a particular category of accounts and pay particular attention to the transactions which may exceed these limits.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. High-risk accounts have to be subjected to intensified monitoring. The Company shall set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

The Company should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures.

CHAPTER-VIII

MISCELLANEOUS

21. Customer Education

The Company shall educate the customer on the objectives of the KYC programme so that customer understands and appreciates the motive and purpose of collecting such information. The Company shall have made KYC guidelines available on website, displayed in branches/ office and prepare specific literature/ pamphlets, etc., which can be made available to customer upon request, to educate the customer about the objectives of the KYC programme.

22. Introduction of New Technologies

The Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering activities as and when online transactions are started/ accepted by the Company.

23. KYC for the Existing Accounts

The Company shall 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.

24. Applicability to branches/offices and subsidiaries outside India

The KYC guidelines shall also apply to the branches/ offices 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/ offices. When local applicable laws and regulations prohibit implementation of these guidelines, the same shall be informed to National Housing Bank/RBI.

25. Record Management

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

- (a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;
- (b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
- (c) make available swiftly, the identification records and transaction data to the competent authorities upon request;
- (d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
- (e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
 - (i) the nature of the transactions;
 - (ii) the amount of the transaction and the currency in which it was denominated;
 - (iii) the date on which the transaction was conducted; and
 - (iv) the parties to the transaction.
- (f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
- (g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

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

25.1 Maintenance of records of transactions

The Company shall maintain proper record of the transactions as required under Section 12 of the PMLA read with Rules 3 of the PML Rules as mentioned below:

- a. All cash transactions of the value of more than rupees ten lacs or its equivalent in foreign currency.
- b. 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.
- c. All transactions involving receipts by non-profit organizations of rupees ten lacs or its equivalent in foreign currency.
- d. 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 has taken place; any such transactions; and
- e. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rule 3 (1) (D).

An Illustrative List of suspicious transaction pertaining to Housing Loan is given in Annexure-III

25.2 Records to contain the specified information

The Company shall maintain records referred to above in Rule 3 of PMLA Rules to contain the following information:

- a) the nature of the transactions;
- b) the amount of the transaction and the denominated currency;
- c) the date on which the transaction was conducted; and
- d) the parties to the transaction.

25.3 Maintenance and preservation of records

Section 12 of PMLA requires every housing finance company to maintain records as under:

- (a) records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules is required to be maintained for a period of ten years from the date of transactions between the clients and the Company.
- (b) records/ documents pertaining to the identification of customers e.g. copies of documents like Passport, Identity Card, Driving Licenses, PAN, Utility bills etc. will be maintained for a period of ten years from the date of cessation of transactions between the customer and the Company.

The Company shall ensure that proper maintenance and preservation of records/ information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required, or when requested by the competent authorities upon request through the Principal Officer.

26. Reporting Requirements to Financial Intelligence Unit - India

26.1 The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information

referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

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

- 26.2 The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility shall be referred to. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. CTR/STR as have been made available by FIU-IND on its website <http://fiuindia.gov.in> .
- 26.3 While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
- 26.4 The Company and its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under paragraph 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

The Principal Officer shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by NHB at the following address:

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

The employees of the Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

The Company and all its Branches / Offices while reporting the STR shall be guided by and follow the guidelines as specified in the 'Guidance Note on Effective Process of STRs Detections And Reporting for Housing Finance Sector, issued by Financial Intelligence Unit – India (FIU), Ministry of Finance in consultation with National Housing Bank dated 30th December, 2015. The Red Flag Indicators (RFI) / Parameters for, STR identification as specified in the subject guidance note being made part of this Policy as Annexure IV for reporting of STRs.

Note: Reports shall be submitted every month by the 15th day of succeeding month; FIU-IND does not accept NIL Cash/ Suspicious Reports if no such transaction occurred during a particular period.

27. Requirements/Obligations under International Agreements/Communications from International Agencies

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

- (a) The “ISIL (Da’esh) & Al-Qaida Sanctions List”, established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at

www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

- (b) The “**Taliban Sanctions List**”, established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at

<https://www.un.org/securitycouncil/sanctions/1988/materials>

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

27.2 Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated 128February 2, 2021 (Annex II of the Master Direction).

27.3 Freezing of Assets under section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 129February 2, 2021 (Annex II of the Master Direction), shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

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

27.5 Jurisdictions that do not or insufficiently apply the FATF Recommendations

- (a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. REs shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
- (b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in (a) & (b) above do not preclude the Company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

- (c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.
- (d) The Company shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

28. Other Measures:

28.1 Secrecy Obligations and Sharing of Information:

- i. The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.
- ii. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
- iii. While considering the requests for data/information from Government and other agencies, REs shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
- iv. An illustrative (but not exhaustive) list of suspicious transaction in housing / builder/project loans is furnished in Annexure – III for guidance of the Housing Finance Companies.

The exceptions to the said rule shall be as under:

- (a) Where disclosure is under compulsion of law,
- (b) Where there is a duty to the public to disclose,
- (c) the interest of the Company requires disclosure and
- (d) Where the disclosure is made with the express or implied consent of the customer.

28.2 CDD Procedure and 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 Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

- a) The Know Your Customer (KYC) / document(s) pertaining to all new individual accounts opened on or after November 01, 2017 have to be invariably uploaded on CKYCR in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

- b) Once KYC Identifier is generated by CKYCR, REs shall ensure that the same is communicated to the individual/LE as the case may be.
- c) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updation as specified in paragraph 38 of the Master Direction, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the RE obtains additional or updated information from any customer as per clause (e) below in this paragraph or Rule 9 (1C) of the PML Rules, the RE shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an RE regarding an update in the KYC record of an existing customer, the RE shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the RE.
- d) The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
- e) For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the RE shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless-
 - (i) there is a change in the information of the customer as existing in the records of CKYCR; or
 - (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - (iii) the validity period of downloaded documents has lapsed; or
 - (iv) the RE considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

28.3 Hiring of Employees and Employee training:

- (a) Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
- (b) The Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.
- (c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

28.4 Quoting of PAN

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

28.5 Selling Third party products:

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

(a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 13(e) of the Master Direction.

(b) transaction details of sale of third-party products and related records shall be maintained as prescribed in paragraph 46 of Chapter VII of the Master Direction.

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

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:

- (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.

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

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

- (a) Persons authorized by the Company for collecting deposits and/ or selling loan related products, their brokers/ agents or the like, shall be fully compliant with the KYC guidelines applicable to the Company.
- (b) All information shall be made available to the National Housing Bank/Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons Authorised by the Company including brokers/ agents etc. who are operating on their behalf
- (c) The books of accounts of persons authorised by the Company including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

28.7 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 will be taken at a Senior Level of and above only after issuing due notice to the customer explaining the reasons for taking such a decision

Digital KYC Process

- A. The Company will develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process will be undertaken only through this authenticated application.
- 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 to authorized officials.
- C. The customer, for the purpose of KYC, shall visit the location of the authorized official or vice-versa. The original OVD shall be in possession of the customer.
- D. Ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application shall put 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 time stamp (HH:MM:SS) on the captured live photograph of the customer.
- E. The Application 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 shall not be used for customer signature. Check that the mobile number used in customer signature shall not be the mobile number of the authorized officer must be ensured.

- 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 RE. 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 RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.
- 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. The authorized officer 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.;
- N. On Successful verification, the CAF shall be digitally signed by authorized officer 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 II

CUSTOMER IDENTIFICATION PROCEDURE FEATURES TO BE VERIFIED AND DOCUMENTS THAT MAY BE OBTAINED FROM CUSTOMERS

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

Provided that,

- 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 licence agreements with such employers allotting official accommodation;
- c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

Officially Valid Documents (OVD) for Identity and Address Check (List A)

Documents	Identity Check	Signature Check	Address Check
Passport	Yes	Yes	Yes
PAN Card	Yes	Yes	No
Voter Id Card	Yes	No	Yes
Driving License	Yes	No	Yes
NREGA Job Card	Yes		
Aadhar Card/ Letter	Yes	No	Yes
Letter issued by the National Population Register containing details of name and address	Yes	No	Yes

Additional Documents as Address Proof (List B)

Sr. No.	Documents
1.	Electric Bill (Not more than 2 months old)
2.	Telephone Bill (Not more than 2 months old)
3.	Post Paid Mobile Bill (Not more than 2 months old)
4.	Piped Gas Bill (Not more than 2 months old)
5.	Water Bill (Not more than 2 months old)
6.	Property or Municipal Tax Receipt
7.	Pension or Family Pension Payment Order
8.	Accommodation Allotment Letter from Employer issued by State/Central Govt Department, Statutory or Regulatory Bodies, PSUs, Scheduled Commercial Banks, Financial Institutions and listed Companies and Leave and License Agreements

Note: 1) 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 OVD so produced by the client with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the Act.

2) The submission of Aadhaar by an individual as a KYC document in cases other than receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act, is not mandatory. However, the individual, if so desires, may provide the same out of his own volition. Customers, at their option, shall submit one of the OVDs.

3) Customer has to submit any one from additional documents as address proof, if OVD doesn't contain current address proof. Customer shall be required to submit updated OVD with current address within a period of three months of the submitting of above documents.

Individual Salaried Customers

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
Identity and Address Proof	➤ Certified Copy of PAN Card/ Form 60 ➤ Certified Copy of any one Document from List A ➤ Certified Copy of any one Document from List B (if OVD doesn't have current address)
Income Proof	➤ Form 16 (Last 2 Years); ➤ Last 2 Years ITRs along with computation, if available; ➤ Last 1 Year Bank Statement for all Bank Accounts;

Sole Proprietary Firms

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
Identity and Address Proof	➤ Certified Copy of PAN Card/ Form 60 of Individual Proprietor ➤ Certified Copy of any one Document from List A of Individual Proprietor

	➤ Certified Copy of any one Document from List B of Individual Proprietor (if OVD doesn't have current address)
<i>Business Proof (Any Two)</i>	➤ Registration Certificate; ➤ Certificate/Licence under Shop and Establishment Act; ➤ GST Certificate; ➤ Importer Exporter Code issued in the name of Proprietary Concern by DGFT ➤ Electric Bill (Not more than 2 months old) ➤ Water Bill (Not more than 2 months old) ➤ Landline Telephone Bill (Not more than 2 months old)
<i>Income and Turnover Proof</i>	➤ Last 3 (Three) Years Complete Income Tax Returns in the name of Sole Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities; ➤ Last 1 (One) GST Return, if registered under GST; ➤ Last 3 (Three) Years Audit Report (if audit is applicable), Balance Sheet, Trading, Profit & Loss and Capital Account duly certified by Chartered Accountant; ➤ Last 1 (One) Year all Banks Account Statements (both Current and Savings);

Note: 1) If two documents of Business Proof are not available, then the Company at its discretion may accept only one of the documents as a proof of business/ activity subject to the contact point verification of the existence of the said business at the mentioned business address.

Legal Entities

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
<i>ID, Address and Business Proof (One Certified Copy of each)</i>	➤ Certificate of Incorporation; ➤ Memorandum and Articles of Association; ➤ PAN Card; ➤ Board Resolution and Power of Attorney granted to its Managers, Officers or Employees to transact on its behalf; ➤ One copy of an OVD containing details of identity and address, one recent Photograph and PAN Card/ Form 60 of the managers, officers or employees as the case may be, holding an attorney to transact on its behalf;
<i>Income and Turnover Proof</i>	➤ Last 3 (Three) Years Complete Income Tax Returns duly authenticated/acknowledged by the Income Tax Authorities; ➤ Last 1 (One) GST Return, if registered under GST; ➤ Last 3 (Three) Years Audit Reports and Financials; ➤ Last 1 (One) Year all current Bank Account Statements;

Partnership Firm

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
<i>ID, Address and Business Proof (One Certified Copy of each)</i>	➤ Registration Certificate; ➤ Partnership Deed; ➤ PAN Card of Partnership Firm; ➤ Partner's Resolution (In case of Partnership Firm is Limited Liability Partnership registered under LLP Act) and Power of Attorney granted to its Managers, Officers or Employees to transact on its behalf; ➤ One copy of an OVD containing details of identity and address, one recent Photograph and PAN Card/ Form 60 of the managers, officers or employees as the case may be, holding an attorney to transact on its behalf; ➤ One copy of an OVD containing details of identity and address, one recent Photograph and PAN Card/ Form 60 of all the Partners; ➤ Proof of Place of Business/ Activity;
<i>Income and Turnover Proof</i>	➤ Last 3 (Three) Years Complete Income Tax Returns duly authenticated/acknowledged by the Income Tax Authorities; ➤ Last 1 (One) GST Return, if registered under GST; ➤ Last 3 (Three) Years Audit Reports (if Audit is applicable) and Financials; ➤ Last 1 (One) Year all current Bank Account Statements;

Trust

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
<i>ID, Address and Business Proof (One Certified Copy of each)</i>	➤ Registration Certificate; ➤ Trust Deed; ➤ PAN Card of Trust; ➤ Trust's Resolution and Power of Attorney granted to its Managers, Officers or Employees to transact on its behalf; ➤ One copy of an OVD containing details of identity and address, one recent Photograph and PAN Card/ Form 60 of the managers, officers or employees as the case may be, holding an attorney to transact on its behalf;
<i>Income and Turnover Proof</i>	➤ Last 3 (Three) Years Complete Income Tax Returns duly authenticated/acknowledged by the Income Tax Authorities; ➤ Last 1 (One) GST Return, if registered under GST; ➤ Last 3 (Three) Years Audit Reports (if Audit is applicable) and Financials;

	➤ Last 1 (One) Year all current Bank Account Statements;
--	--

Unincorporated Association or a Body of Individuals

FEATURES TO BE VERIFIED	DOCUMENTS (BRIEF LIST OF DOCUMENTS GIVEN BELOW)
<i>ID, Address and Business Proof (One Certified Copy of each)</i>	➤ PAN Card of unincorporated association or body of individuals; ➤ Formation Documents (e.g. Partnership Deed etc.); ➤ Resolution of the managing body of such association or body of individuals; ➤ Power of Attorney granted to transact on its behalf ➤ One copy of an OVD containing details of identity and address, one recent Photograph and PAN Card/ Form 60 of the managers, officers or employees as the case may be, holding an attorney to transact on its behalf;
<i>Income and Turnover Proof</i>	➤ Last 3 (Three) Years Complete Income Tax Returns duly authenticated/acknowledged by the Income Tax Authorities; ➤ Last 1 (One) GST Return, if registered under GST; ➤ Last 3 (Three) Years Audit Reports (if Audit is applicable) and Financials; ➤ Last 1 (One) Year all current Bank Account Statements;

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

**SUSPICIOUS TRANSACTIONS PERTAINING TO HOUSING LOANS
(ILLUSTRATIVE LIST)**

- a) Customer is reluctant to provide information, data, documents;
- b) Submission of false documents, data, purpose of loan, details of accounts;
- c) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc.
- d) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
- e) Approaches a branch/office of Company, which is away from the customer's residential or business address provided in the loan application, when there is branch/office nearer to the given address;
- f) Unable to explain or satisfy the numerous transfers in the statement of account/ multiple accounts;
- g) Initial contribution made through unrelated third party accounts without proper justification;
- h) Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
- i) Suggesting dubious means for the sanction of loan;
- j) Where transactions do not make economic sense;
- k) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
- l) Encashment of loan amount by opening a fictitious bank account;
- m) 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;
- n) Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
- o) Multiple funding of the same property/dwelling unit;
- p) Request for payment made in favor of a third party who has no relation to the transaction;
- q) 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.
- r) Multiple funding/ financing involving NGO/ Charitable Organisation/ Small/ Medium Establishments (SMEs)/ Self Help Groups (SHGs)/ Micro Finance Groups (MFGs)
- s) Frequent requests for change of address;
- t) Overpayment of installments with a request to refund the overpaid amount

**II. SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER/ PROJECT LOANS
(ILLUSTRATIVE LIST)**

- a) Builder approaching Company for a small loan compared to the total cost of the project;
- b) Builder is unable to explain the sources of funding for the project;
- c) Approvals/sanctions from various authorities are proved to be fake.

RED FLAGS / PARAMETERS TO IDENTIFY STR**List of RED FLAG INDICATORS (RFI) for STR identification:**

In order to facilitate an effective reporting regime of STRs by HFCs, the note identifies a list of RFIs that may be further identified as a Suspicious Transaction and then reported as a STR, upon due verification.

The RFIs are identified as situations that may be encountered by HFCs in particular and are categorized under the following broad categories:

- a. Customer Centric;
- b. Transaction / Loan Account Centric;
- c. Property / Property document Centric; and
- d. Cases (falling under a, b & c above) that would require auto reporting
- e. List of RFIs pertaining to builder/project loans

As such the suggested RFIs are essentially situations that would require further analysis as they have the potential of being a STR. The Principal Officers are expected to sensitise the respective HFCs of the RFIs and should there be adequate justification, the RFIs may then be reported as STRs to the Principal Officer for further reporting to the FIU. Mere sighting of the enumerated situations is not expected to be reported as a STR on an “as is” basis as the same is in the nature of possible trigger of reporting as a STR and should be accordingly reported after adequate diligence and with proper justification.

As indicated above, the note also identifies situations that may generate Auto triggers within the system of a HFC which may automatically be referred to the respective Principal Officer for reporting as a STR.

There are certain parts (as specifically indicated) that would need to be assessed by each HFC, in lines of its business practises, and determine the point of trigger of the RFI for the said HFC. Upon such identification, all HFCs are expected to approve the RFIs by their Board and incorporate the same as a part of their respective KYC policy.

Thus in order to ensure effective reporting of STRs, the note identifies the following transactions/situations as RFIs which (upon adequate diligence and justification) may be identified as a Suspicious Transaction and then onward reported as a STR.

Part A: RFIs that are Customer Centric:

Sr. No.	Sub- Category	Types
1.	Identity of Customer	a. Submission of false Identification Documents. b. Customer holding multiple PAN. c. Identification documents which could not be verified within reasonable time or replaced with another set of Identification documents. d. Accounts opened with names very close to other reputed business entities. e. Customer uses aliases and a variety of similar but different addresses. f. Customer spells his or her name differently from one transaction to another, without justification. g. Name of customer indicated differently in different KYC documents enabling creation of multiple customer identities. h. A customer/company who is reluctant or refuses to provide complete information, data, documents and to reveal details about its activities or to

		provide financial statements /Employment related documents / KYC documents. Doubt over the real beneficiary of the loan account i. The customer is reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons. j. The customer approaches a branch/office of a HFC, which is away from the customer's residential or business address provided in the loan application, when there is HFC branch/office nearer to the given address. k. Changes in mailing address of the Customer more than [twice]* in last 6 months l. Unusual capital, partnership, management or employment structure of companies compared to other institutions in the same sector or general company structure. m. Current data not updated with relevant regulatory authorities, without justification. n. Existing or new partners/shareholders abstaining from giving information about their personal and commercial background, having indications that they did not have interest, education or experience in the field in which the company operates
2.	Background of a customer	a. The customer details matched with watch lists (e.g. UN list, Interpol list etc.) b. Notice/Letter from a law enforcement agencies / Regulators/ Other Government Agencies: In case of such notices received, Principal Officer should be informed for further action /advise on the matter. This notice shall be treated as an alert to analyse the transactions in such accounts and if the transactions appear to be suspicious the same should be included in the STR along with the details mentioned in the "Ground of Suspicion". These Accounts are to be reported even if they are closed. c. Adverse Media / Public News: Branches / offices should check for adverse media coverage with the names of the customer. The names of customers that are pointed as suspects or accused in such reports shall be searched and in case of matches the same may be further internally analyzed for reporting purposes. d. Customer shows income from "foreign sources" on loan application without providing proper documentation.
3.	Credit bureau Information	a. Multiple addresses reflecting against the name of the customer which has not been shared / or does not match with the employment history / residence details provided.

Part B: RFIs that are Transaction / Loan Account Centric:

Sr. No.	Sub- Category	Types
1.	Multiple Accounts	a. Use of Bank A/c's of Third Parties for payment of EMIs at more than [*] occasions. b. Change in the bank account from which PDC/ ECS are issued more than [*] in last [6/12*] months c. Total amount of payments through DD, Cash and 3rd party Cheques valued at [*] EMIs / part payments in last 30 days d. Customer appears to have recently established a series of new relationships with different financial entities.
2.	Nature of Activity in an Account	a. Unusual activity compared with past transactions. b. Encashment of loan amount by opening a fictitious bank account. c. Activity inconsistent with what would be expected from declared business/profile of the customer. d. Part closure to the extent of [*] % or more of the loan amount in one or more occasions within 6 months. e. Loan Accounts with original tenor of more than 1 year are foreclosed within 6 months after disbursal of loan. f. 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. g. Overpayment of instalments in cash with a request to refund the excess amount. h. Customer conducts transactions at different physical locations in an apparent attempt to avoid detection. i. Customer presents confusing details about the transaction or knows only few details about its purpose. j. Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account. k. Account indicated by customer to receive interest payment against a deposit placed is attached by Government Authorities
3.	Nature of transactions	a. Unusual or unjustified complexity shown in a Transaction that may normally be done in simpler manner. b. Initial contribution made through unrelated third party accounts without proper justification; c. No economic rationale or bonafide purpose behind the transaction. d. Availing a top-up loan and/or equity loan, without proper justification of the end use of the

		loan amount e. Suggesting dubious means for the sanction of loan or placing a deposit. f. PAN not disclosed but multiple deposits raised (across branches to avoid TDS).
4.	Value of transactions	a. Value just under the reporting threshold amount in an apparent attempt to avoid reporting. b. Multiple related cash transactions which are broken to just below the following thresholds: i) Rs. 50,000/- in a day ii) Rs. 10,00,000/- in a month c. Value inconsistent with the client's apparent financial standing. d. Deposits made in cash amounting to Rs[*]and above and without details of source.
5.	Transaction amongst family members	Transaction between members of the same family to avail a loan wherein there is no genuine transaction / rationale.
6.	Transaction more than specified percentage of the EMI , paid in cash by a Delinquent Borrower.	Delinquent borrower for more than 6 months repays the loan in cash beyond [twice]* the original EMI.

(*): to be decided by respective HFC at the Board level and should be a part of the KYC policy of the HFC duly approved by the Board.

Part C: RFIs that are Property/Property Document Centric:

Sr. No.	Sub- Category	Types
1.	Cash payment indicated in the Sale Deed/Agreement	Cash payment shown as consideration paid to the seller for purchase of a property and the source of which cannot be explained or proof not provided by the customer.
2.	Valuation of property	Valuation of property shown considerably lower in the sale deed than the government approved rate / RESIDEX, especially on sale deeds executed within a period of 12 months.
3.	Change in Ownership without rationale	Converting/changing the individual properties in the name of Company/Trust/HUF/Partnership Firm/LLP by executing a sale deed at a low price or by way of any type of agreement , attorney, arrangement (registered or not) and subsequently in quick succession further transaction is shown at a considerably higher amount in favour of third parties.
4.	Refusal to share own Contribution details	Specifically in cases where the source is specified as "Funds from Family" and the customer fails or refuses to divulge any information or proof on where the concerned family member is providing the funds from.
5.	Property repurchased	Customer buys back a property that he or she recently sold without justification

Part D : RFIs that may be considered to be auto generated through a system

Sr. No.	Scenario	Indicator/ Trigger
1.	Foreclosure by a customer in a very short period	Loan Accounts with original tenor of more than 1 year are foreclosed within 6 months after disbursal

		of loan.
2.	Frequently change in repayment bank account during currency of account	Change in the bank account from which PDC/ ECS are issued more than [*] in last [6/12] months
3.	Negative information about customer through external sources/ database or Notice received from any Agency / Regulator/ Other Government Agencies	a. The customer details matched with watch lists (e.g. UN list, Interpol list etc.) b. Notice/Letter from a law enforcement agencies / Regulators/ Other Government Agencies: In case of such notices received, Principal Officer should be informed for further action /advise on the matter. This notice shall be treated as an alert to analyse the transactions in such accounts and if the transactions appear to be suspicious the same should be included in the STR along with the details mentioned in the “Ground of Suspicion”. The Accounts are to be reported even if they are closed. c. Adverse Media / Public News: Branches / offices should check for adverse media coverage with the names of the customer. The names of customers that are pointed as suspects or accused in such reports shall be searched and in case of matches the same may be further internally analyzed for reporting purposes.
4.	Frequent change of Address without reasonable explanation	Changes in mailing address more than [twice]* in last 6 months
5.	Account having a large volume of repayments by depositing DD, Cash and 3rd party Cheques	Total amount of payments through DD, Cash and 3 rd party Cheques valued at [*] EMI's / part payments in last 30 days
6.	Transaction more than specified percentage of the EMI, paid in cash by a Delinquent Borrower.	Delinquent borrower for more than 6 months repays the loan in cash beyond [twice]* the original EMI.
7.	Cash transactions	Multiple related cash transactions which are broken to just below the following thresholds: i) Rs.50,000/- in a day ii) Rs.10,00,000/- in a month
8.	Part payments	Part closure to the extent of [*] % or more of the loan amount in one or more occasions within 6 months.
9.	Separate bank accounts	Use of Bank A/c's of Third Parties for payment of EMI's at more than [*] occasions.

(*) : to be decided by respective HFC at the Board level and should be a part of the KYC policy of the HFC duly approved by the Board.

Part E : Additional List of RFIs pertaining to Builder/Project Loans:

- Builder approaching the HFC for a small loan compared to the total cost of the project-;
- Builder is unable to explain the sources of funding for the project;
- Approvals/sanctions from various authorities are proved to be fake;
- Builder retains substantial number of the Units in the Project in his or his family members names
- Builder has known political connections / shareholders or directors of his company are individuals with suspicious background
- Frequent Reconstitution of partnership/ proprietorship without justification.
- Allotting different numbers to the same flat in different style/order.