

The Last Amended in 152nd Board Meeting Dated 19.11.2024



Know Your Customer [KYC] & Anti Money Laundering [AML] Policy

INDEX

Contents

Sr. No.	Particulars	Page No.
	Omnibus Clause	03
1.	Chapter - I: Introduction	03
2.	Chapter – II: General	11
3.	Chapter – III: Customer Acceptance Policy	13
4.	Chapter – IV: Risk Management	14
5.	Chapter – V: Customer Identification Procedure (CIP)	16
6.	Chapter -VI: Customer Due Diligence (CDD) Procedure	17
7.	Chapter - VII: Record Management	27
8.	Chapter VIII: Reporting Requirements	28
9.	Chapter IX: Requirements/Obligations under International Agencies	28
10.	Chapter – X: Other Measures	29
11.	Annexure - I: Digital KYC Process	33
12.	Annexure - II: Illustrative list of STRs pertaining to Builder/Project/Corporate Clients	35

KNOW YOUR CLIENT AND ANTI MONEY LAUNDERING POLICY

Omnibus Clause

Particulars	Directions
Applicable RBI directions / circulars / notifications	<p>a. Master Direction - Know Your Customer (KYC) Direction, 2016, as amended from time to time</p> <p>b. The contents of this Policy shall stand automatically amended in case of any amendments / revisions issued by the Reserve Bank of India ("RBI") from time to time.</p>
Approval Authority	The Company's 'Know Your Customer' (KYC) Policy will be duly approved by its Board of Directors or any committee of the Board to which power has been delegated

CHAPTER – I

1. Introduction

In terms of the provisions of prevention of Money Laundering Act 2002 (hereinafter referred to as Money Laundering Act, 2002 and rules framed thereunder, wherein Cent Bank Home Finance Limited (hereinafter referred to as CBHFL) needs to comply with the statutory obligations of adhering to the prescriptions made therein. Based on these statutory requirements, National Housing Bank issued Policy to all Housing Finance Companies (HFCs) for adherence to these requirements. Accordingly, CBHFL (Company) formulated a policy on the subject and amended the same from time to time.

Reserve Bank of India (RBI) vide its press release dated August 13, 2019 on Transfer of Regulation of HFCs to RBI, advised that Housing Finance Companies (HFCs) will be treated as one of the categories of Non-Banking Financial Companies (NBFCs) for regulatory purposes and RBI will carry out a review of the extant regulatory framework applicable to the HFCs and come out with revised regulations in due course.

RBI has since advised extending the Master Direction- Know Your Customer (KYC) Direction, 2016 to Housing Finance Companies vide its Circular DOR.NBFC (HFC).CC No.111/03.10.136/2019-20 dated May 19, 2020. Hence, the RBI Master Direction – Know Your Customer (KYC) Direction, 2016 Ref. No. DBR.AML.BC. No.81/14.01.001/2015-16 dated February 25, 2016, updated from time to time and last updated on January 04, 2024, are now applicable to Housing Finance Companies and the instructions/ guidelines/ regulations contained in the circulars issued by National Housing Bank stands repealed.

In view of the above, the existing Policy has been reviewed by incorporating the latest RBI guidelines and provisions of the PML Rules and Act, and renamed as Know Your Customer (KYC) and Anti Money Laundering Policy.

2. Applicability

CBHFL's KYC Policy is applicable to all types of customers including individuals, partnership firms, employees, corporate entities, associations, trusts, societies and juridical persons. This policy also covers the Natural and Juridical persons who are the ultimate beneficiaries of the credit facilities extended by the Company and the natural persons who represent such persons or entities. The policy is also applicable to the persons authorized by CBHFL including brokers/ agents etc.

3. Definitions

In this policy, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them under the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

3.1 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);

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

3.3 "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 (BO)

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

Explanation- For the purpose of this sub-clause-

1. Controlling ownership interest" means ownership of/entitlement to more than 25 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 15 per cent of capital or profits of the partnership.

c. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals. Explanation: Term ‘body of individuals’ includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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 authorised 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:

- a. authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- b. branches of overseas banks with whom Indian banks have relationships,
- c. Notary Public abroad,
- d. Court Magistrate,
- e. Judge,
- f. Indian Embassy/Consulate General in the country where the 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 “Company” shall mean Cent Bank Home Finance Limited.

3.8 “Designated Director” shall mean a person designated by the Company to ensure overall compliance with the obligations imposed under the PML Act and PML Rules

3.9 “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.

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

3.11 “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.

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

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

3.14 (a) “Officially Valid Document” (OVD) means

Sr. No.	Officially Valid Documents
1.	Passport
2.	Driving License
3.	Voter’s Identity Card issued by Election Commission of India
4.	Proof of possession of Aadhaar Number i.e. Aadhaar Letter, Aadhaar Letter downloaded from UIDAI website (e-Aadhaar), Aadhaar Card, Aadhaar Secure QR Code, Aadhaar Paperless Offline e-KYC (an XML document generated by the UIDAI) *
5.	Job Card issued by NREGA duly signed by an officer of the State Government
6.	Letter issued by the National Population Register containing details of Name, Address of the customer with photograph of the card holder
*Ensure to redact/ blacken only the first eight digits of Aadhaar No. (on copy of Aadhaar Letter/ Aadhaar Card obtained).	

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:-

Sr. No.	Deemed Officially Valid Documents (DOVD)
i.	Utility bill, in the name of the client, 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 & License Agreements with such employers allotting official accommodation
In case a client submits Deemed to be OVD (DOVD) towards Current Address, client must submit an OVD mentioned in (A)(3), updated with Current Address, within three months of submission of the DOVD.	

- 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.

3.15 Offline verification” shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

3.16 “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)

3.17 “Principal Officer” means the officer designated by the Company for the purpose of this Policy

3.18 “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.

3.19 “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.

3.20 Terms bearing meaning assigned in this Policy, unless the context otherwise requires, shall bear the meanings assigned to them below:

- i. “Common Reporting Standards” (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
- ii. “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.
- iii. “Walk-in Customer” means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.
- iv. “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner.
- v. “Customer identification” means undertaking the process of CDD.
- vi. “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.
- vii. “IGA” means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
- viii. “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- ix. “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company.
- x. “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that they are consistent with the customers’ profile and source of funds.
- xi. “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.
- xii. “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.

xiii. “Regulated Entities” (REs) means

- a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (St CBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as ‘banks’
- b. All India Financial Institutions (AIFIs)
- c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
- d. Asset Reconstruction Companies (ARCs)
- e. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
- f. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xiv. “Shell Bank” means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

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

xvi. Wire transfer means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and

regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER -II

General

4. This policy shall enable the Company to know/understand its customers and their financial dealings better which will enable carrying out the operations and manage the risks prudently and thereby prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Hence, it becomes incumbent on all the staff members to understand the Policy and adhere to the Policy stipulated herein with letter and spirit.
5. **The key elements of the Policy shall include the following:-**
 - a. Customer Acceptance Policy (CAP)
 - b. Risk Management
 - c. Customer Identification Procedure (CIP); including Customer Due Diligence (CDD) and
 - d. Monitoring of Transactions

5A. 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 shall 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 of the Company, in alignment with the outcome of the risk assessment exercise. However, it shall be reviewed annually.

(c) The outcome of the exercise shall be put up to Audit Committee of the Board, and should be available to competent authorities and self-regulating bodies.

5B. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall have Board approved policies, controls and procedures in this regard. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

6. Designated Director:-

- a. The Board of Directors of the Company hereby nominates Managing Director as 'Designated Director' 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, including changes from time to time shall be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).
- c. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
- d. The Principal Officer shall not be nominated as Designated Director

7. Principal Officer:-

- a. The Managing Director shall appoint a Principal Officer of the level of General Manager or above.
- b. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations.
- c. The Principal Officer shall act independently and shall report directly to the MD & CEO / Designated Director.
- d. The name, designation and address of the Principal Officer, including changes from time to time, shall be communicated to the Director, FIU-IND.
- e. The Company may engage any agency for verification of KYC documents for authenticity besides verification by own employees. However, the decision making functions of determining compliance with KYC norms shall not be outsourced.

8. The Company shall ensure compliance with the KYC Policy through:

(i) The below mentioned officials shall constitute as Senior Management and will be responsible for effective implementation of KYC policies and procedures:

- Chief Risk Officer
- Chief Credit & Operations
- Business Heads (for their respective business)
- Chief Compliance Officer

(ii) Independent evaluation of the compliance functions of CBHFL policies and procedures, including legal and regulatory requirements will be carried out.

(iii) Concurrent/Internal Audit system to verify the compliance with KYC/AML policies and procedures.

(iv) Submission of quarterly audit notes and compliance to the Audit Committee.

The Company shall not outsource the decision-making functions for determining compliance with KYC norms.

CHAPTER - III

Customer Acceptance Policy (CAP)

9. The Company has framed a customer acceptance policy in the form of the Credit Policy of the Company.

10. The Company shall ensure that:

- a. No account is opened in anonymous or fictitious/benami name.
- b. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- c. No transaction or account-based relationship is undertaken without following the CDD procedure.
- d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified.
- e. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.
- f. The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer desires to open another account or avail any other product or service from the Company, there shall be no need for a fresh CDD exercise as for as identification of the customer is concerned.
- g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
- h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is

clearly spelt out.

- i. Suitable system shall be put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
- j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- k. 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).
- l. Where Goods and Services Tax (GST) details are available, the GST number must be verified from the search/verification facility of the issuing authority.

11. The Company shall ensure that the 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.

11A. Where Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

CHAPTER - IV

Risk Management

12. For Risk Management, the Company shall have a risk based approach which includes the following.

- a. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the Company.
- b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in as given below:

This AML /Risk based categorization of a Customer is mentioned below, subject to any regulatory

requirement as may be specified from time to time:

<p>Low</p> <p>Partnership Firm (Regd. Deed).</p>	<p>Low Risk individual customers are those individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and the transactions with them by and large conform to known profile. These include following:</p> <ol style="list-style-type: none"> 1. Salaried Employee 2. Self Employed Professional 3. Govt. Dept & Govt. Owned Companies 4. Limited Companies (Public & Private) 5. Farmer 6. Transport Driver 7. Street Vendor 8. Fisherman 9. Daily wage Worker 10. Artisan 11. Homemaker 12. All loan cases up to Rs. 25 Lakhs. 13. All individual deposits up to Rs. 100 Lakhs
<p>Medium</p>	<ol style="list-style-type: none"> 1. Retailers 2. Manufacturers 3. Traders 4. Sole Proprietorships 5. SMEs/MSMEs 6. Large Enterprises 7. Partnerships: Multiple owners. 8. Proprietorships Firm 9. Partnership Firm 10. Law Firm 11. Corporate Firm 12. Proprietorships 13. Partnership 14. Registered body 15. Travel Agency 16. Blind 17. Purdanashin 18. Advocate 19. Others
<p>High</p>	<ol style="list-style-type: none"> 1. Trust 2. Society 3. NGO 4. Law Firm 5. NPO(Non-Profit Organization) 6. Fund Manager 7. Charities 8. Broker 9. Association/ Clubs 10. NBFC 11. Minor 12. HUF (Hindu Undivided Family) 13. PEP (Political Exposed Person) 14. HNI Deposit of more than 1 Cr 15. Non face to face Customer

	<p>16. Unclaimed</p> <p>17. Loans to NRIs</p> <p>18. Freelancer</p> <p>19. Contractor</p> <p>20. Cooperative Society</p> <p>21. Others</p> <p>22. Politically Exposed Persons (PEP)</p> <p>23. Family members and close relatives of PEP</p> <p>24. Very high cash transactions (Rs. 10 Lakhs and above and</p> <p>25. suspicious transactions reported to FIU-IND Persons with dubious reputation as per public information available.</p> <p>26. High Net worth Individuals {HNI}. HNI for this purpose shall mean individuals whose annual income is equal & more than Rs. 60 lakh per annum.</p> <p>27. Non-face to face meeting with customers or dubious persons.</p>
--	---

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same may be specified in the Credit Policy.

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

CHAPTER - V

Customer Identification Procedure (CIP)

13. Customer identification shall mean identifying the customer and verifying his/ her / its identity by using reliable, independent source documents, data or information while establishing a relationship.

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

- (a) Commencement of an account-based relationship with the customer.
- (b) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained
- (c) Selling third party products as agents such as insurance products, selling our own product and any other product for more than rupees fifty thousand.
- (d) When the Company has reason to believe or having a suspicion that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may 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 Company to satisfy itself 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 including done by a third party and undertaking enhanced due diligence measures, as applicable, rest with the Company.

CHAPTER- VI

Customer Due Diligence Procedure (CDD)

Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

15. For undertaking CDD, 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; 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; and

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

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

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof 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 Annex I.

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 Annex I.

v) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR in accordance with Section 23.

Provided 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 audit on the functioning of KYC. 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.

Explanation 2: 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.

16. 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:

i. 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 and can only carry out Offline Verification of Aadhaar for identification.

ii. 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. 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.

v. 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.

vi. 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.

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. 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 liveness check in order to guard against spoofing and such other fraudulent manipulations.

ix. 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.

x. 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.

xi. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. The Company endeavor 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.

xiii. The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

Part II - CDD Measures for Sole Proprietary firms

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

18. 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
- 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.

19. 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 branch official undertake contact point verification and collect such other information and

clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part – III CDD Measures for Legal Entities

20. 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 above relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

21. 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 above relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

22. 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 above relating to beneficial owner, managers, officers or employees, as

the case may be, holding an attorney to transact on its behalf

23. 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 above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
- 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 1: Unregistered trusts/partnership firms shall be included under the term ‘unincorporated association’.

Explanation 2: Term ‘body of individuals’ includes societies.

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

- a. Document showing name of the person authorised to act on behalf of the entity;
- b. Documents, as specified above, 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.

Part - IV Identification of Beneficial Owner

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

- (a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any

shareholder or beneficial owner of such companies.

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

Part – V On-going Due Diligence

- 26.** 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.
- 27.** The extent of monitoring shall be aligned with the risk category of the customer with High risk accounts are subjected to more intensified monitoring.
- 28.** A system of periodic review of risk categorisation of accounts, with such periodicity being **at least once in six months**, and the need for applying enhanced due diligence measures shall be put in place.

29. Periodic Updation

Periodic updation shall be carried out **at least once in every two years** for **high risk** customers, **once in every eight years** for **medium risk** customers and **once in every ten years** for **low risk** customers as per the following procedure:

a) Individual Customers:

- i) **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.
- ii) **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels (such as online banking / internet banking, mobile application of Company), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiv) of Directions, for the purpose of proof of address, declared by the customer at the time of updation/periodic updation.

iii) Accounts of customers, who were minor at the time of opening account, on their becoming major:

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

b) Customers other than individuals:

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

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

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

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

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

Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

In order to ensure customer convenience, Company may consider making available the facility of periodic updation of KYC at any branch.

The Company shall not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder / holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

The Company shall ensure to provide acknowledgment with date of having performed KYC updation.

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

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

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

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

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

Part – VI Enhanced Due Diligence and Simplified Due Diligence Procedure

31. Accounts of non-face-to-face customers (other than Aadhaar OTP based on- boarding):

the Company will ensure that the first payment/ disbursal is to be effected through the customer's KYC complied account with another Company, for enhanced due diligence of non-face-to-face customers.

32. Accounts of Politically Exposed Persons (PEPs)

A. The Company shall have the option of establishing a relationship with PEPs provided that:

- a. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
- b. the identity of the person shall have been verified before accepting the PEP as a customer;
- c. the decision to open an account for a PEP is taken at a senior level in accordance with the Customer Acceptance Policy;
- 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;
- f. the CDD measures as applicable to PEPs including enhanced monitoring on an on- going basis are applicable.

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

33. Client accounts opened by professional intermediaries:

The Company shall ensure while opening client accounts through professional intermediaries, that:

- a. Clients 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 its discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

f. The ultimate responsibility for knowing the customer lies with the Company.

CHAPTER -VII

Record Management

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

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

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

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

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

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

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

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

(g) maintain records of the identity and address of their customer, and records in respect of transactions

referred to in Rule 3 in hard or soft format.

CHAPTER-VIII

Reporting Requirement to Financial Intelligence Unit – India (FIU-IND)

- 35.** The Company shall furnish to the Director, FIU – IND the information in respect of prescribed transactions 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 reporting entities 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.

- 36.** The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The Company understands that while furnishing information to FIU-IND, the delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation.
- 37.** 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.
- 38.** Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

CHAPTER – IX

Requirements/obligations under International Agreements

Communications from International Agencies

- 39.** The Company shall ensure that 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).

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

The procedure laid down in the UAPA Order dated 5 March 14, 2019 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

41. Jurisdictions that do not or insufficiently apply the FATF Recommendations

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

CHAPTER – X

Other Instructions

42. Secrecy Obligations and Sharing of Information:

- a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the lender and customer.
- b) Information collected from customers for the purpose of opening of loan 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 getting the express permission of the customer.
- c) While considering the requests for data/information from Government and other agencies, the Company shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in transactions.
- d) The exceptions to the said rule shall be as under:
 - i. Where disclosure is under compulsion of law
 - ii. Where there is a duty to the public to disclose,
 - iii. the interest of bank requires disclosure and
 - iv. Where the disclosure is made with the express or implied consent of the customer

43. 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. The Company shall upload the Know Your Customer (KYC) data with CERSAI in respect of new individual accounts opened on or after April 01, 2017.

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

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

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

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

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

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

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

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

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time.

2. In addition to the above, other United Nations Security Council Resolutions (UNSCRs) circulated by Reserve Bank of India in respect of any other jurisdictions /entities from time to time shall also be taken note of.

45. Selling Third party products

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

46. Hiring of Employees and Employee training

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

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

- (a) Persons authorised by the Company for selling loan related products and their brokers/agents or the like, shall be fully compliant with the KYC Policy applicable to the Company.
- (b) All information shall be made available to the National Housing Bank and Reserve Bank of India to verify the compliance with the KYC Policy and accept full consequences of any violation by the persons authorised by the Company including brokers/agents etc. who are operating on our behalf.

48. Statutory Policy

1. The Company shall ensure that the provisions of PML Act and the rules framed thereunder and the Foreign Regulation (Regulation) Act, 2010, wherever applicable, shall be adhered to strictly.
2. 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 may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken by the Principal Officer.

49. Independent Evaluation of compliance of KYC Policy

Internal Audit / Concurrent Audit shall evaluate the system of effectiveness of the KYC Policy and procedures and verify the compliance with KYC Policy / AML Measures and report to Top Management on an annual basis.

50. Quarterly Reporting to ACB

The Company shall place a note containing review on adherence to KYC norms and AML measures to Audit Committee of the Board on quarterly basis.

51. Conclusion

Notwithstanding anything contained in this Policy, the Company shall ensure compliance with any additional requirements as may be prescribed under the provisions of PML Act or rules thereunder or any other law or instructions given by RBI as applicable to the Company from time to time. Any change / amendment in applicable laws / notifications as above shall be deemed to be incorporated in the Policy and this Policy shall be deemed to have been amended and revised accordingly.

CBHFL KYC POLICY

Digital KYC Process

A. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.

B. The access of the Application shall be controlled by the Company and it shall be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

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

D. The Company shall ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee ID number and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

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

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

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

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

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

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

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

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

CBHFL KYC POLICY

A. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER / PROJECT/ CORPORATE CLIENTS:

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

B. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO INDIVIDUALS:

- 1) Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- 2) Unnecessarily complex client structure.
- 3) Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
- 4) Customer is reluctant to provide information, data, documents;
- 5) Submission of false documents, data, purpose of loan, details of accounts;
- 6) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
- 7) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
- 8) Approaches a branch/ office, 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;
- 9) Unable to explain or satisfy the numerous transfers in account/ multiple accounts;
- 10) Initial contribution made through unrelated third party accounts without proper justification;
- 11) Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount;

- 12) Suggesting dubious means for the sanction of loan;
- 13) Where transactions do not make economic sense;
- 14) Unusual financial transactions with unknown source.
- 15) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- 16) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
- 17) Encashment of loan amount by opening a fictitious bank account;
- 18) 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;
- 19) Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
- 20) Multiple funding of the same property/dwelling unit;
- 21) Request for payment made in favour of a third party who has no relation to the transaction;
- 22) 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.
- 23) Multiple funding / financing involving NCO / Charitable Organisation / Small/ Medium Establishments (SMEs) / Self Help Groups (SHCs) / Micro Finance Groups (MFCs)
- 24) Frequent requests for change of address;
- 25) Overpayment of instalments with a request to refund the overpaid amount.
- 26) Investment in real estate at a higher/lower price than expected.
- 27) Clients incorporated in countries that permit bearer shares.

Company Secretary