SUNDARAM HOME

Policy Name	KYC & AML Policy	Version No.	1.12
Date of Approval	20th June 2006	Date of last revision	01-Feb-2024
Department Responsibile	Operations	Date of next revision	-

Version History

Version No.	Recommended By	Approved By	Approval / Revision date	Description / Description of change
1.0	-	Board of Directors	20-Jun-2006	KYC & AML Policy
1.1	-	Board of Directors	25-Jan-2011	In compliance with, the regulatory guidelines issued by the National Housing Bank (NHB) through its circular NHB/ND/DRS/Pol-No. 33/2010-11 dated 11 October 2010
1.2	-	Board of Directors	30-Jan-2015	Principal Officer & Designated Director included
1.3	-	Board of Directors	17-Jul-2017	Inclusion of "e-Aadhaar" as a proof of identity and address in Annex II of the Company's Policy
1.4	-	Board of Directors	21-May-2019	Amendments made as per the Revised Guidelines on KYC policy
1.5	-	Board of Directors	24-Jan-2020	No change
1.6	-	Board of Directors	20-May-2020	Designated Mr. Lakshminarayanan Duraiswamy as the Designated Director for the purpose of Anti-Money Laundering (AML) compliances under Prevention of Money Laundering Activities (PMLA) effective 01st April 2020

1.7	**-**	**Board of Directors**	**25-Jan-2021**	**No change**
1.8	**-**	**Board of Directors**	**4-Feb-2022**	**No change**
1.9	**-**	**Board of Directors**	**14-May-2022**	**Mr. R. Venkatasubramanian, Company Secretary, appointed as the Principal Officer of the Company effective responsible for monitoring and reporting all transactions and sharing of information as required under the law**
1.10	**-**	**Board of Directors**	**29-Mar-2023**	**No change**
1.11	**-**	**Board of Directors**	**26-Oct-2023**	**Amendments made as per the Revised Guidelines on KYC policy**
1.12	**-**	**Board of Directors**	**1-Feb-2024**	**Amendments made as per the Revised Guidelines on KYC policy**

SUNDARAM HOME FINANCE LIMITED
Registered Office: 21 Patullos Road, Chennai – 600 002

POLICY ON 'KNOW YOUR CUSTOMER' AND 'ANTI-MONEY-LAUNDERING' MEASURES

A. Introduction

1. This Policy is based on, and is in compliance with, the regulatory guidelines issued by the Reserve Bank of India (RBI) through its Master Direction - Know Your Customer (KYC) Directions, 2016, (as updated from time to time) to all Regulated Entities. The Act and Rules apply to HFCs as much as to banking companies, other financial institutions and intermediaries without distinction. As a HFC, the Company's primary business is the provision of term loans for housing in India. The Company also extends loans on the security of immovable property for personal or commercial purposes. The Company accepts term deposits from the public but within a regulated framework. Such deposits represent a small proportion of the Company's resources.

   The Company does not offer a wide range of financial products and services such as those offered by a commercial bank or a financial conglomerate. Unlike a commercial bank, the Company cannot accept demand deposits withdrawable by cheque, draft, and order or otherwise and it cannot open or maintain current or savings accounts. The Company does not extend overdraft or cash-credit facilities or collect or discount bills for customers. Also, unlike banks, the Company does not undertake money transfers, such as through bank drafts or electronic transfers. It does not dispense cash through electronic machines or issue credit cards. The Company has no subsidiaries in India or abroad and does not have overseas operations.

2. Given its specialised and limited roles and functions, the Company is unlikely in practice to encounter several of the types of situations or enter into some of the types of business or non-business relationships captured by the Act and the Rules. Thus, not all of the requirements of the Act and the Rules that would seem to apply to, say, a commercial bank would be equally applicable to the Company in the ordinary course of its business. Nevertheless, this Policy incorporates the requirements, too, to conform to the wide statutory and regulatory ambit. In practice, the staff concerned should carefully exercise their reasonable judgment in determining whether particular situations or circumstances encountered by them fall within the purview of this Policy and need any appropriate action as required, while ensuring that the Policy is unfailingly implemented in all cases where it is clearly applicable.

3. The Company shall ensure that the provisions of the Act, the Rules framed thereunder, and the Foreign Contribution (Regulation) Act, 2010, wherever applicable, is adhered to strictly. In case of any inconsistency between this Policy and the statutory and regulatory requirements, the latter shall prevail.

4. In this Policy, unless repugnant to the subject or context:

a. words importing the masculine gender shall include the feminine; and
b. words in the singular shall include the plural, and *vice versa*.

B. "Know Your Customer" (KYC) Policy

The primary objective of the Policy is to protect the Company from being used, intentionally or unintentionally for money-laundering activities or other financial crimes. The KYC/AML norms and procedures will also enable the Company to understand the customers and their financial dealings better and manage the related risks prudently.

Further the Policy shall ensure compliance with The Prevention of Money-Laundering Act, 2002 (PML Act), read with the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time together with other applicable regulatory provisions so as to protect the Company against threats arising from money laundering, terrorist financing, proliferation financing, and other related risks. The Policy will also enable the Company to adopt the best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

Definitions:

i. **"Aadhaar number"** means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth the 'Aadhaar Act';

ii. **"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;

iii. **"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.

iv. **Beneficial Owner (BO):**

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

Explanation - For the purpose of this sub-clause:-

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

(ii) *"Control" 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 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "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.
Explanation- Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. **"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:

- 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.

vi. **"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.

vii. **"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.

viii. **"Customer"/"Person"** means 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)

and 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.

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

x. **"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 (as per the definition of Companies Act'2013) duly authorized by the Board of Directors.

xi. **"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.

xii. **"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).

xiii. **"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.

xiv. **"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.

xv. **"Group"** – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

xvi. **"Group Policy"** – In terms of PML Rules, the Company's implementation of group wide programmes including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

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

xviii. **"Non-profit organization"** means an entity or organization 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.

xix. **"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.

xx. **"Officially Valid Document" (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and 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:-

- utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- property or Municipal tax receipt;
- pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- 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.

xxi. **"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).

xxii. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the Company's knowledge about the customers, customers' business and risk profile and source of funds/wealth.

xxiii. **"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.

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

xxv. **"Principal Officer"** means the Chief Compliance Officer (CCO) & Company Secretary of the Company.

xxvi. **"Suspicious transaction"** means a transaction referred to in rule 2(1)(h) of the Rules, 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 thereof; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no 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.

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

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

xxviii. **"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 SHFL by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

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

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

All other expressions unless defined herein shall have the same meaning as have been 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.

C. CUSTOMER ACCEPTANCE POLICY & RISK ASSESSMENT

1. In line with the RBI's master direction – Know Your Customer (KYC) direction, the company has formulated Customer Acceptance Policy which lays down the broad criteria for acceptance of customers.

   (i) No account will be opened with the Company in an anonymous or fictitious or benami name.

   (ii) Parameters of risk perception will be clearly defined in terms of the customer's location, clients and mode of payments, volume of turnover, and social and financial status, to enable categorisation of customers into low-, medium-, and high-risk categories.

   (iii) The Company will specify the documentation requirements and other information to be collected in respect of different categories of customers while opening their accounts, depending on their perceived risk categorisation and keeping in mind the statutory and regulatory requirements.

   (iv) The Company shall not open a new account, and may close an existing account, where the Company is unable to apply appropriate customer due diligence measures, eg, where the Company is unable to verify the identity of the applicant/customer or obtain the documents required as per the risk categorisation owing to non-co-operation of the applicant/customer or non-reliability of the information furnished by him to the Company. The Company shall consider filing a Suspicious Transaction Report (STR), if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer. However, suitable safeguards will be built into the procedures to avoid harassment of the applicant/customer. The decision to close an account will be taken at a senior level, after giving due notice to the customer, indicating the reason for such a decision.

(v) Where a customer acts on behalf of another person or an entity, as where an account is operated by a mandate holder or is opened by an intermediary in a fiduciary capacity, the attendant circumstances shall be clearly spelt out in conformity with the established law and practices.

(vi) Before opening a new account, the Company will carry out necessary checks to ensure that the customer's identity does not match that of:
(a) any person who is known as a terrorist or has a criminal background within the knowledge of the Company, or
(b) a banned entity such as a terrorist organization, or
(c) whose name appears in the sanctions lists issued by UN Security Council circulated by National Housing Bank and the sanctions lists circulated by Reserve Bank of India, as indicated in Chapter IX of the KYC Master Direction.

2. The nature and extent of the information to be collected and the due diligence to be carried out by the Company while opening an account for a new customer will depend on its perception of the risk involved in entertaining him and dealing with him as a customer. However, staff should not adopt an intrusive approach, and should only seek such information from the customer as is relevant to the risk category and is in conformity with the regulatory guidelines.

3. For each new customer, a customer profile will be compiled, based on his risk categorisation, and containing information relating to his identity, social/financial status, nature of business activity, his clients and their location, etc. The contents of the customer profile shall be treated as confidential and, to the extent that these are not in public knowledge, shall not be divulged for cross- selling or any other purpose without the customer's consent. Any other information may be sought from the customer, with his consent, after the opening of the account.

   For the purpose of risk categorisation, individuals [other than high net-worth individuals (HNIs)] and entities whose identities and sources of wealth can be easily known and transactions in whose accounts, by and large, conform to the known profile, may be categorised as low risk. Such customers include: salaried employees with well-defined salary structures, persons belonging to the lower economic strata of the society whose accounts show small balances and low turnover, government departments and government-owned companies, regulators, and statutory bodies. In such cases, only the basic requirements of verification of the customer's identity and location need be met.

4. A customer likely to pose a higher-than-average risk to the Company may be categorized as a medium- or high-risk customer, depending on his background, nature and location of activity, country of origin, sources of funds, and client profile. In such a case, especially where the sources of the customer's funds are not clear, enhanced due diligence measures may be applied in respect of specified transactions based on the risk assessment. Such customers may include:
   a. non-resident customers,
   b. HNIs,
   c. trusts, charities, non-government organisations, and organisations receiving donations,
   d. companies having close family shareholding or beneficial ownership,
   e. firms with 'sleeping partners',

f. politically exposed persons (PEPs) of foreign origin,
g. non-face-to-face customers, and
h. those with dubious reputation as per available public information.

Where an existing customer or the beneficial owner of an existing account subsequently becomes PEP, the Managing Director's approval would be necessary to continue the business relationship with him. If continued, the relationship shall be subjected to enhance 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.

Enhanced Due Diligence (EDD) in respect of specified transactions shall include:

a. Verification of the Identity by the authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 or any other prescribed process;
b. Examination of the ownership and financial position, including the sources of funds;
c. Recording the purpose behind conducting the specified transactions and the intended nature of the relationship between the transacting parties; and
d. Maintenance of information obtained while applying EDD for a period of 5 years from the date of the transaction.

   Prevention of specified transactions where the client is unable to fulfill the conditions under EDD;

   Enhanced monitoring and greater scrutiny in the case of specified transaction(s) that are considered suspicious or likely to involve proceeds of crime.

   For the purpose of this Policy, "specified transaction" means — (a) any withdrawal or deposit in cash, exceeding such amount; (b) any transaction in foreign exchange, exceeding such amount; (c) any transaction in any high value imports or remittances; and (d) such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

5. The company shall not undertake any transaction or account-based relationship without complying the CDD procedures.

6. The company shall obtain the additional / optional information only with the explicit consent of the customer post the transaction is completed or account is opened.

7. The company shall follow the CDD procedure for all the joint account holders as well while opening a joint account.

8. The company shall verify the Permanent Account Number (PAN) wherever obtained from the verification facility of the issuing authority.

9. A Unique Customer Identification Code (UCIC) shall be allocated while entering into a new relationship with customers.

10. The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC complaint of the company desires to avail addition loan or desires to open additional account, there shall be no need for fresh CDD exercise.

11. 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).

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

13. It shall be ensured that adoption and implementation of the Customer Acceptance Policy does not become too restrictive as would result in denial of the Company's services to the general public, especially to those who are financially or socially disadvantaged.

D. CUSTOMER IDENTIFICATION PROCEDURE

1. At the time of commencement of an account–based relationship, the customer's identify shall be verified and information obtained on the purpose and intended nature of the business relationship he seeks with the Company.

2. In the case of an account based or *non-account-based relationship, the customer's identity shall be verified while carrying out:

   a. a single transaction of Rs. 50,000 or more, or a series of several transactions that appear to be connected and total Rs. 50,000 or more; or
   b. any international money transfer.

3. All reasonable steps shall be taken to verify the identity of any beneficial owner of an account.

4. Where the customer is a judicial person, the identity and authority of any person purporting to act on its behalf shall be verified.

5. The company shall ensure that introduction is not to be sought while opening accounts.

6. Customer identification means identifying the customer and verifying his identity by using reliable, independent source documents, and information. Sufficient information needs to be obtained to establish, to the Company's satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the proposed relationship. Documents and information shall be obtained as indicated in **Annex I**.

7. When a doubt arises about the authenticity, veracity, or the adequacy of previously obtained customer identification data, the matter should be referred, where the account is maintained at a branch, to the head of the branch and, where the account is maintained at the Corporate Office, to the Head (Operations) as the case may be.

*In practice, the Company is unlikely to enter into such a relationship.

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

E. Customer Due Diligence (CDD) Procedure

A) CDD Procedure for Individuals -

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:

(i) Recent coloured passport size photograph

(ii) Copy of PAN (Form 60 as per IT rules to be taken in case Pan is not available)

(iii) Copy of Aadhaar or one of the OVDs as defined above to be taken for verification of the identity and the address OR the equivalent e-document thereof; and
(a) 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
(b) he decides to submit his Aadhaar number voluntarily to a bank or any company notified under first provision to sub-section (1) of section 11A of the PML Act;

(iv) The KYC Identifier with an explicit consent to download records from CKYCR

(v) Other documents including in respect of the nature of the business and financial status of the customer or the equivalent e-document thereof, as may be required by the company.

Note -

Offline Verification of Aadhaar – If Offline Verification of Aadhaar is adopted, the company may carry offline verification of Aadhaar if customer is desirous of undergoing offline verification for identification purpose. However, if customer submits his Aadhaar copy, the company will ensure such customer to blackout the Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under Section 7 of the Aadhaar Act.

If the customer provides an equivalent e document of any OVD, the company should verify the digital signature as per the provisions of the IT Act,2000 and any rules made thereunder and take a live photo as specified under Digital KYC process defined below.

The company may also carry out KYC verification under digital KYC process as defined below –

Digital KYC Process

If digital KYC process is adopted as part of process, the company will follow the requirements and ensure compliance -

a) An authenticated application will be used at customer points for completing KYC of their customers.

b) The access of the Application shall be controlled by the company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by 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) It will be ensured 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 Code (assigned by the company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

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

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 the customer's own mobile number. Upon successful validation of the OTP, it will be treated as a customer signature on CAF. However, if the customer does not have his/her own mobile number, then the mobile number of his / her family / relatives / known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of the Authorized Official should not be used for customer signature. The company will check that the mobile number used in the customer signature shall not be the mobile number of the Authorized Official.

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

k) Subsequent to all these activities, the Application should give information about the completion of the process and submission of activation request to the activation officer of the company, and also generate the transaction-id / reference-id number of the process. The Authorized Official shall intimate the details regarding transaction-id/reference-id number to the customer for future reference.

l) The Authorized Official should check and verify that: (i) information available in the picture of the document is matching with the information entered by the Authorized Official in CAF. (ii) live photograph of the customer matches with the photo available in the document. and (iii) all of the necessary details in CAF, including mandatory field, are filled properly.

m) On successful verification, the CAF shall be digitally signed by the Authorized Official, who will take a print of CAF, get signatures / thumb-impression of customers at an appropriate place, then scan and upload the same in the system. Original hard copy may be returned to the customer.

Simplified procedure for opening accounts of Individuals

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

a) The Company shall obtain a self-attested photograph from the customer.

b) The authorized officer of the company should certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

c) The account shall remain operational initially for a period of 12 months, within which CDD, as prescribed above, should be carried out.

d) Balances in all their accounts taken together shall not exceed Rs.50,000/- at any point in time.

e) The total credit in all the accounts taken together shall not exceed Rs.1,00,000/- in a year.

f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case of Directions (d) and (e) above are breached by him.

g) When the balance reaches Rs.40,000/- or the total credit in a year reaches Rs.80,000/-, the customer shall be notified that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

h) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established by undertaking CDD or V-CIP.

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

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. 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 (v) below is complete.
iii. the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
iv. 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.
v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
vi. 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.
vii. A 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, SHFL shall clearly indicate that such accounts are opened using OTP based e-KYC and other 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. viii. SHFL 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.

Video Customer Identification Process (V-CIP):

The company may undertake V-CIP to carry out the following, whenever this gets implemented:

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 Section 28, 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 Section 17.
iii) Updation/Periodic updation of KYC for eligible customers.

The following minimum standards shall be adhered to:

(a) V-CIP Infrastructure:

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

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

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

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

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

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

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

viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

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

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

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

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

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

vi) The authorised official of the company performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
   a) OTP based Aadhaar e-KYC authentication
   b) Offline Verification of Aadhaar for identification
   c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
   d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

   The company shall ensure to redact or blackout the Aadhaar number in terms of Section 16. 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 three working days from the date of carrying out V-CIP.

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

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

viii) The company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

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

x) The authorised official of the company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

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

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

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

B) 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.

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.

(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) Legal Entity Identifier Code Certificate (where aggregate exposure from Banks and Financial Institutions is Rs. 5 crore and above).

(h) 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.

(i) Utility bills such as electricity, water, landline telephone bills, etc.

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

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

C) CDD Measures for Legal Entities

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

a) Certificate of incorporation

b) Memorandum and Articles of Association

c) Permanent Account Number of the company

d) Legal Entity Identifier Code Certificate (where aggregate exposure from Banks and Financial Institutions is Rs. 5 crore and above)

e) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

f) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

g) The names of the relevant persons holding senior management position; and

h) he registered office and the principal ix) The place of its business, if it is different.

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

a) Registration certificate

b) Partnership deed

c) Permanent Account Number of the partnership firm

d) Legal Entity Identifier Code Certificate (where aggregate exposure from Banks and Financial Institutions is Rs. 5 crore and above)

e) 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

f) The names of all the partners and

g) Address of the registered office, and the principal place of its business, if it is different.

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

a) Registration certificate.

b) Trust deed

c) Permanent Account Number or Form No.60 of the trust.

d) Legal Entity Identifier Code Certificate (where aggregate exposure from Banks and Financial Institutions is Rs. 5 crore and above)

e) 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

f) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust

g) the address of the registered office of the trust; and

h) list of trustees and documents, as specified in a&b, for those discharging the role as trustee and authorised to transact on behalf of the trust.

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

a) Resolution of the managing body of such association or body of individuals;

b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.

c) Legal Entity Identifier Code Certificate (where aggregate exposure from Banks and Financial Institutions is Rs. 5 crore and above)

d) Power of attorney granted to transact on its behalf;

e) 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

f) Such additional information as may be required by the Company, to collectively establish the legal existence of such an association or body of individuals.

Explanation:

1) Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.

2) Term 'body of individuals' includes societies.

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

a) Document showing name of the person authorised to act on behalf of the entity;

b) Documents, as specified in Section 16, 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. Additional information, where such information requirement has not been specified in the internal KYC Policy is obtained with the explicit consent of the customer.

Provided that in case of a Trust, the Trustees shall disclose their status at the time of commencement of an account-based relationship or when carrying out following transactions:

- International money transfer operations for a person who is not an account holder of the Company.
- For a non-account based walk-in customer, where the amount involved is equal to or exceeds Rs.50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
- When the Company has a 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 Rs.50,000/-

F. Monitoring of transactions

Ongoing due diligence shall be exercised with respect to the business relationship with every customer. The transactions with every customer shall be closely examined in order to ensure that they are consistent with the company's knowledge of the customer, his business and risk profile. The company shall have systems and procedures for monitoring its customers' accounts, based on the risk categorisation, the size of the transactions entered into by the company with the customers, their background, such as the country of his origin, sources of his funds, the types of transaction involved, and other risk factors. For this purpose, staff shall seek to understand the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk-sensitivity of the account. Special attention shall be paid to all complex and unusually large transactions and all unusual patterns that seem to have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract attention. High-risk accounts shall be subjected to intensified monitoring. The risk categorization of accounts and the need for applying enhanced due diligence measures to particular accounts shall be reviewed periodically.

G. Money Laundering and Terrorist Financing Risk Assessment

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 customers, 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 from time to time.

b) Risk Assessment done by the company are properly documented and it is done 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.

d) The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. The Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of the business. Further, it shall monitor the implementation of the controls and enhance them if necessary.

H. The company's Compliance function shall carry out an independent evaluation of the Company's KYC & AML Policy and procedures, including compliance with the legal and regulatory requirements. The internal and concurrent auditors shall specifically check and verify the application of KYC & AML procedures at the branches and other offices and comment on any observed lapses. The main findings of the audits shall be put up to the Audit Committee regularly. Accountability will be fixed for serious lapses and intentional circumvention of prescribed procedures and guidelines.

I. The company's employee-training program will include a focus on adequate training of relevant staff in KYC procedures, with appropriate differentiation of frontline staff, compliance staff and staff dealing with new customers, so that all those concerned fully understand the rationale behind the KYC Policy and implement it consistently.

J. Customer education

Implementation of KYC procedures may involve asking customers to provide information that may be of a personal nature or that has not been asked for previously. Some customers may question the need for and the purpose of collecting such information. The company shall train its staff concerned to deal with such situations and seek to educate the customer about the objectives of the KYC program with the help of appropriate literature put out by the Company.

K. Introduction of new technology

The company shall pay special attention to any money-laundering threats that may arise from a new or developing technology, including on-line transactions that might favour anonymity, and take measures, if needed, to prevent their use in money-laundering schemes.

L. The Designated Director

Mr. Lakshminarayanan Duraiswamy, Managing Director shall be the Designated Director for the purpose of compliance with Chapter IV of the Act.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

M. The Principal Officer

Mr. R. Venkatasubramanian, Chief Compliance Officer & Company Secretary shall be the Principal Officer of the Company responsible for monitoring and reporting all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies and any other institution involved in the fight against money-laundering and financing of terrorism.

The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

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

N. Periodic Updation

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

a) 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 categorised 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) Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Mobile number for Aadhaar authentication should be same as the one available with them in the customer's profile, in order to prevent any fraud
   vi) 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 bona-fides. Normally, OVD/consent forwarded by the customer through mail/post, etc., shall be acceptable.

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, ATMs, digital channels (such as online banking / internet banking, mobile application of SHFL), 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, ATMs, digital channels (such as online banking / internet banking, mobile application of SHFL), 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, the company, may, at their option, obtain a copy of OVD or deemed OVD as defined in Section 3(a)(xiv) or the equivalent e-documents thereof, as defined in Section 3(a)(x)), for the purpose of proof of address, declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the company in their internal KYC policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated.

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:

i) **No change in KYC information:** In case of no change in the KYC information of the Legal Entity customer, a self-declaration in this regard shall be obtained from the Legal Entity customer through its email id registered with the company, ATMs, digital channels (such as online banking / internet banking, mobile application of the company), letter from an official authorized by the Legal Entity 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.

ii) **Change in KYC information:** In case of change in KYC information, the company shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

c) Additional measures:

In addition to the above, the company shall ensure that,

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

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

iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, 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.

iv) In order to ensure customer convenience, company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated.

v) The company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the company where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated.

vi) The company shall ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

In order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the company the update of such documents within 30 days of the update to the documents for the purpose of updating the records in the company.

In case of existing customers, the company shall obtain the PAN 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 PAN 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 PAN 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 to the company that he does not want to submit his PAN 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 – "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.

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.

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 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.

(b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

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.

O. Maintenance of records of transactions

1. The Company shall have a system of maintaining proper records of transactions as mentioned below:

   a. all cash transactions of the value of more than Rs. 10 lakh or its equivalent in foreign currency;

   b. all series of cash transactions integrally connected to each other which have been valued below Rs. 10 lakh or its equivalent in foreign currency where the transactions have taken place within a month and the aggregate value of such transactions exceeds Rs. 10 lakh;

   c. all transactions involving receipts by non-profit organizations of value of more than Rs. 10 lakh or its equivalent in foreign currency;

   d. all cash transactions where, to the Company's knowledge, forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions; and

   e. all suspicious transactions, whether or not made in cash.

2. The company shall maintain proper records of all cash transactions (deposits and withdrawals) of Rs. 10 lakh and above. The internal monitoring system shall have an in-built procedure for fortnightly reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to the controlling unit or the head office.

3. Records referred to above shall contain the following information:
   a. the nature of the transaction;
   b. the amount and currency of the transaction;
   c. the date on which the transaction was conducted; and
   d. the parties to the transaction.

4. The company shall maintain records for discharging obligations under the provisions of Chapter IV of the Act which shall include the following:

   a. records of all transactions referred to in section 12 of the Act read with Rule 3 of the Rules shall be maintained for a period of five years from the respective dates of the transactions with the customers; and
   b. records of documents evidencing the identity of the clients and beneficial owners, as well as account files and business correspondences relating to clients during the course of the business relationship and for a period of five years after the business relationship is ended or the account has been closed whichever is later; and
   c. Providing access to information that may be sought by the Authority and maintaining the confidentiality of the same; and

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

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

P. Reporting to the Financial Intelligence Unit-India (FIU-IND)

a) The company shall report information on transactions referred to in section 12(1) of the Act read with Rule 3 of the Rules relating to cash and suspicious transactions *direct* to:

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

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

The Company, 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 Section 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

Copies of the information furnished to the Director shall be retained by the Principal Officer for the purposes of official record. **Annex II** contains an illustrative (but not exhaustive) list of suspicious transactions.

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 this Policy.

(b) All information shall be made available to the National Housing Bank 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.

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 HFCs 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.

b) The Company shall also endeavour to install 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.

Q. Secrecy Obligations and Sharing of Information

The company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the company and customer.

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.

While considering the requests for data/information from Government and other agencies, banks 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.

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, the interest of the Company requires disclosure and
c. Where the disclosure is made with the express or implied consent of the customer.

Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

R. Sharing KYC information with Central KYC Records Registry (CKYCR)

The company will capture the KYC information / details as per KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

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

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

T. Introduction of New Technologies

The company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, the company shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

U. Selling Third Party products

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

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

(b) transaction details of sale of third party products and related records shall be maintained as prescribed in Section 46 of Chapter VII (Record Management).

(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 debit to customers' account or against cheques; and obtaining and verifying the PAN given by the account-based as well as walk-in customers.

V. Quoting of PAN

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

W. Hiring of Employees and Employee training

Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.
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.

X. Adherence to the KYC and AML guidelines by the Company's agents / Brokers

The Company's agents or persons authorized by it, for its business, will be required to be compliant with the applicable KYC & AML Guidelines.

All requisite information shall be made available to the RBI / National Housing Bank to verify the compliance with the applicable KYC & AML Guidelines.

The books of accounts of persons authorized by the company, including agents, etc., so far as they relate to the business of the company, shall be made available for audit and inspection whenever required.

The company shall accept full consequences of any violation by the persons authorised by NBFCs/RNBCs including brokers/agents etc. who are operating on their behalf.

Y. Internal Audit

Concurrent / Internal audit system to verify the compliance with KYC / AML policies and procedures.

The audit findings and compliance thereof will be put up before the Board of Directors or any committee of the Board to which power has been delegated.

Z. No outsourcing of decision-making function

The company shall not be outsourcing decision-making functions to ensure compliance with KYC norms.

Annex I

CUSTOMER IDENTIFICATION REQUIREMENTS: INDICATIVE GUIDELINES

A. Trust / nominee / fiduciary accounts

There exists the possibility that trust/nominee/fiduciary accounts can be used to circumvent the customer identification procedures. Where a customer is acting on behalf of another person as a trustee/nominee or is an intermediary, the Company may insist on receipt of satisfactory evidence of the identity of the intermediary and of the person(s) on whose behalf he is acting, and details of the nature of the trust or other arrangements in place. While opening an account for a trust, reasonable precautions should be taken to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a foundation, steps should be taken to verify the founder-managers/directors and the beneficiaries, if defined. If a decision is taken to accept such an account in terms of the Customer Acceptance Policy, reasonable measures should be taken to identify the beneficial owner(s) and verify his/her/their identity so that the Company comes to know who the beneficial owner(s) is/are.

B. Accounts of companies and firms

The staff should be vigilant against business entities being used by individuals as a 'fronts' for maintaining accounts with the Company. The legal status of the legal person/entity should be verified through proper and relevant documents. The identity and authority of any person purporting to act on behalf of the legal/juridical person/entity should be verified. The control structure of the entity should be examined, the source of its funds determined, and the natural persons who have a controlling interest and who comprise the management identified. These requirements may be moderated according to the risk perception; for instance, in the case of a public company it will not be necessary to identify all the shareholders.

C. Client accounts opened by professional intermediaries

When it is within the Company's knowledge, or there is reason to believe, that a customer's account opened by a professional intermediary is on behalf of a client, that client must be identified. Where the 'customer due diligence' is carried out by an intermediary, the staff concerned should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

D. Accounts of politically exposed persons (PEP)

Politically exposed persons (whether as Customer or Beneficial Owner) are individuals who are or have been entrusted with prominent public functions by a foreign countryincluding the heads of states or of governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, and important political party officials. If and when a person of this category, or a member of his family, or his close associate, seeks to establish a relationship with the Company, sufficient information on the person, including information available in the public domain, shall be gathered. The identity of the person should be verified, and information should be asked for about the sources of his funds/wealth **and that of his/her family members or close associates** before accepting him as a customer. The decision to open an account for such a person should only be taken by the Senior Management. 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. Any such account should be put through enhanced monitoring on an ongoing basis.

E. Accounts of non-face-to-face customers

In the case of non-face-to-face customers, in addition to the usual customer identification procedures, specific and adequate procedures will be applied to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of overseas customers, given the difficulty of matching the customer with the documentation provided, reliance may be placed on introduction by an acceptable third party or on authentication by, eg, a regulated and supervised bank or other financial institution.

Annex II

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 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;
9) Unable to explain or satisfy the numerous transfers in the statement of account/ multiple accounts;
10) Initial contribution made through unrelated third party accounts without proper justification;

11) Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
12) Suggesting dubious means for the sanction of loan;
13) Where transactions do not make economic sense;
14) 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 NGO / Charitable Organisation / Small/ Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs)
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.