Subject: **KYC & AML Policy**	Original Issue Date: 08.11.2010	Version No.: 7.0
	Last revision date: 06.05.2026	

HOME FIRST FINANCE COMPANY INDIA LIMITED

('Home First')

KNOW YOUR CUSTOMER

&

ANTI-MONEY LAUNDERING POLICY

[KYC & AML]

KYC & AML Policy

Chapter I - PRELIMINARY

1. INTRODUCTION

This Know Your Customer (KYC) and Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) Policy ("Policy") is framed in accordance with the provisions of the *Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025*, including amendments issued by the Reserve Bank of India from time to time.

The Policy has been adopted by HomeFirst (hereinafter referred to as the "Company") with the objective of establishing robust processes to identify and verify customers, understand the nature of their financial dealings, and monitor transactions on an ongoing basis. This enables the Company to manage risks prudently and safeguard itself from being used, intentionally or unintentionally, for money laundering, terrorist financing, or other illicit activities. This Policy is also aligned with the applicable provisions of the Prevention of Money Laundering Act, 2002 (PMLA), and the rules and guidelines issued thereunder, as amended from time to time.

2. OBJECTIVES OF POLICY

The key objectives of the KYC and AML Policy are as under:

a. To establish a regulatory compliant KYC mechanism to on-board customers
b. To ensure compliance throughout the life-cycle of customers as per the laid down norms;
c. To prevent the Company's business channels/products/services from being used as a channel for Money Laundering ("**ML**")/ Terrorist Financing ("**TF'**);
d. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
e. To ensure compliance with the laws and regulations in force from time to time;
f. To protect the Company's reputation;
g. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

3. Applicability: This Policy shall be applicable to all verticals/products of the Company and its authorized representatives, whether existing or to be rolled out in future.

4. Definition: For the purpose of this Policy, definition of various terms used shall be as under:

1. **"Central KYC Records Registry" ("CKYCR")** means a reporting entity, substantially owned and controlled by the Central Government, and authorized by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client in such manner and to perform such other functions as may be required under the PML Rules.
2. **"Customer"** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
3. **"Designated Director"** means, as defined under rule 2(ba) of the PML Rules. the Managing Director or a whole-time Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the PML Rules.
4. **"Officially Valid Document" (OVD)** means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card

issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that:

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:
    - 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.

5. **"Principal Officer"** or **"PO"** means, as defined under rule 2(f) the Rules, an officer at the management level designated by the Board of Directors of the Company for overseeing and managing the KYC and AML Policy and related procedures. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
6. **"Suspicious Transaction"** means, as defined under rule 2(g) of the PML Rules, a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
    a. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved; 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.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or 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.

CHAPTER II - Know Your Customer's Standards

HomeFirst's KYC policy framework seeks to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, the Company may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

5. **Key Elements of the Policy:** As per RBI Directions, HFCs should frame their KYC policies incorporating the following four key elements:

    a. Customer Acceptance Policy;
    b. Customer Identification Procedures;
    c. Monitoring of Transactions; and
    d. Risk Management

6. **Designated Director:** The Company has appointed the Managing Director & CEO of the Company as the "Designated Director" in terms of the Prevention of Anti- Money Laundering (Amendment) Rule 2013. The Designated Director shall be responsible for overall compliance under PMLA and Rules and Regulation made thereunder. The name of the Designated Director, his designation, address and contact details including changes from time to time, shall be communicated to the Director, FIU-IND and RBI, as applicable.

7. **Principal Officer:** The Company has designated Chief Risk Officer of the Company as "Principal Officer." The name of the Principal Officer so designated, his designation, address and contact details including changes from time to time, shall be communicated to the Director, FIU-IND and RBI, as applicable.The Principal Officer shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.

8. **Compliance of KYC Policy:**
    The Company shall undertake the following steps to ensure compliance with KYC Policy:
    a. Internal audit system to verify the compliance with KYC/AML policies and procedures.
    b. Submission of quarterly audit notes and compliance to the Audit Committee.
    c. Independent evaluation of the compliance to the KYC-AML policy.
    d. "Senior Management Team" for the purpose of KYC compliance
    ''Senior Management Team" comprises of the Managing Director & Chief Executive Officer, Chief Risk Officer, Head-Internal Audit, Chief Compliance Officer, Team Lead/Head – Operations, Process, Customer Service and such other officials that the MD & CEO may determine from time to time depending upon their functional roles and responsibilities.

    The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER III - CUSTOMER ACCEPTANCE POLICY (CAP)

The Company has formulated a robust Customer Acceptance Policy which aims to verify the identity and address of customer by using reliable, independent source documents, data, or information.

9. HomeFirst's Customer Acceptance Policy, which lays down explicit criteria for acceptance of customers, ensures the following aspects of the customer relationship:

a. No account is opened in anonymous or fictitious/benami name.
b. No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
c. No transaction or account-based relationship is undertaken without following the CDD procedure.
d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
e. Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, is obtained with the explicit consent of the customer.
f. The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of HomeFirst desires to open another account with the Company, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account
h. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
i. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India from time to time.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
k. Where an equivalent e-document is obtained from the customer, HomeFirst shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
l. Where GST number is available, the same shall be verified through the search/verification facility provided by the issuing authority.
m. HomeFirst should not refuse to extend financial facilities to members of the general public, particularly individuals who are financially or socially disadvantaged, including Persons with Disabilities (PwDs). Applications for onboarding or periodic KYC updates shall not be rejected without due consideration, and the responsible officer must properly document the reasons for any such rejection
n. Where 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.

CHAPTER IV – RISK MANAGEMENT

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

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

a. The Company shall categorize its customers into **low**, **medium**, and **high-risk** category, based on the KYC risk assessment and risk perceived by the Company.
b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
   Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC Policy.
c. The Company may also use the FATF Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association (IBA), and other agencies, etc., in its risk assessment.

d. 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.

Given the nature of our business and its focus on the lower income section of the society, the Company shall categorize the customers according to the risk perceived and factors mentioned below:

I. Low Risk: Individuals and Entities whose identities and sources of wealth can easily be identified and transaction in whose accounts by and large confirm to the known profile come under this category.

a. All Formal Salaried customers whose salary structures are well defined and receiving salary in account
b. People belonging to government department and government owned companies, Public Sector Units, Public Limited Companies, Private limited Companies and Multinational companies.
c. Self-employed customers with proper income documents such as ITR, P&L, Balance Sheet etc.
d. People belonging to lower economic strata of the society whose accounts show small balances and low turnover.
e. Self Employed customers with no formal documents like ITR, P&L, Balance Sheet etc. and less than INR 50,000 monthly assessed income.
f. Salaried applicants with variable income/unstructured income, receiving salary in cash/cheque less than INR 50,000 monthly assessed income.

II. Medium Risk: Individuals or entities whose source of wealth can be established through reference checks and verification**.**

a. Salaried applicants with variable income/unstructured income, receiving salary in cash/cheque more than INR 50,000 monthly assessed income.
b. Self-employed customers with a sound business where we can verify with suppliers/customers as to nature and volume of transactions as well as credibility in business dealings. No formal documents like ITR, P&L, Balance Sheet etc. and above INR 50,000 monthly assessed income.
c. Self Employed customers with no formal documents like ITR, P&L, Balance Sheet etc. and above INR 50,000 monthly assessed income. These customers are with a sound business where we can verify with suppliers/customers as to nature and volume of transactions as well as credibility in business dealings.

III. High Risk: Individuals or entities that pose a higher-than-average risk to the Company will be categorised as high-risk customers. This will be ascertained at the time of credit underwriting after looking at the customers background, nature of business/employment, predictability of cash flows etc. Examples of high-risk customers requiring higher due diligence may include:

a. Non-resident customers
b. High net worth individuals with income above 5 lakh per month
c. Trusts, charities, NGOs and organizations 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. Those with dubious reputation as per available public information, etc

CHAPTER V - Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information to the satisfaction of the Company. The Company shall obtain sufficient information such as Voter ID card, PAN number, Passport etc., to its satisfaction, to establish the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship.

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

a. Commencement of an account-based relationship with the customer.
b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. Selling third party products as agents, selling their own products and any other product for more than INR 50,000.
d. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds INR 50,000, whether conducted as a single transaction or several transactions that appear to be connected.
e. When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of INR 50,000.
f. Introduction shall not be sought while opening accounts.

It will be ensured that due diligence is observed based on the risk profile of the customer in compliance with the extant guidelines in place and the same will be available for verification. Besides risk perception, the nature of information/ documents required will also depend on the type of customer (individual, corporate etc.). For each customer the Company has to obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. The representatives of the Company collect identity proof, bank account details and property documents and verifies the same at different levels along with the applicant's occupation, residence and other documents as applicable.

CHAPTER- VI CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

12. Procedure for obtaining identification

Customer Due Diligence means to identify the clients, verify their identity, obtaining information on the purpose and intended nature of the business relationship, having regard to the ML/TF risks identified and the size of business, using reliable and independent sources of identification. The following CDD measures shall be undertaken at the time of commencement of an account-based relationship with the customer.

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose, and intended nature of the business relationship, where applicable;
b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

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

13. Policy Guidelines for CDD if the Customer is an Individual

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:

For CDD of an individual, the Company shall carry-out the following activities:

a. One recent photograph of the customer to be obtained.

b. **Permanent Account Number ("PAN")** or the equivalent e-document thereof shall be obtained. If PAN has not been obtained by the customer, then Form No. 60 as defined in Income-tax Rules, 1962 shall be taken.

c. **Officially Valid Documents ("OVD" or "KYC documents")** to be obtained- In addition to the above, certified copy of one of the OVDs or the equivalent e-document thereof or one of the following shall be taken for verification of the identity and the address:

i. The Aadhaar Number where:
- The customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act; or
- The customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company is notified under first proviso to sub-section (1) of Section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI; or

ii. Proof of Possession of Aadhaar number where offline verification can be carried out; or

iii. Proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or

iv. If a customer submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then the Company shall retrieve the KYC records from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless:
- there is change in the information of the customer vis-à-vis that existing in the records of CKYCR; or
- the current address of the customer is required to be verified; or
- the respective credit approving authority of the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer; or
- the validity period of documents downloaded from the CKYCR has lapsed.

d. **Other requirements to be complied with respect to various KYC documents**

a. <u>Aadhaar number may specifically be obtained in the following scenarios</u>:

- If customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act; or
- If a customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company is notified under first proviso to sub-section (1) of Section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI.

b. <u>Authentication using e-KYC authentication facility provided by the UIDAI</u> - As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI (under first proviso to sub-section (1) of Section 11A of the PMLA), it may conduct such authorization and use the e-KYC facility in accordance with

the conditions prescribed under the Aadhaar Act/ RBI KYC Directions. Further, in such a case, if a customer wants to provide a current address, different from the address as per the identity information available in Central Identities Data Repository of the UIDAI, he/she shall provide a self-declaration to that effect to the Company.

c. If the customer submits his/ her Aadhaar number, the Company will ensure that such customers redact or blackout his/ her Aadhaar number, where the authentication of Aadhaar number is not required under Section 7 of the Aadhaar Act.
d. The use of Aadhaar, proof of possession of Aadhaar etc. shall be in accordance with the Aadhaar Act and other applicable regulations/ rules.
e. In case proof of possession of the Aadhaar has been submitted by a customer, the Company shall carry out offline verification wherever possible.
f. Where a customer has submitted an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and take a live photo as specified under the Digital KYC Process as specified below.
g. Where a customer submits any OVD or proof of possession of Aadhaar number and its offline verification of such OVD/ proof of possession of Aadhaar cannot be carried out, the Company shall have option to carry-out verification through the process prescribed for Digital KYC Process in the subsequent paragraph.

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.

Part II - CDD Measures for Proprietor / Partnership / HUF/ Club/Trust / Societies /Unincorporated association or a body of individuals/ Limited Companies are:

- Proof of legal existence
- Proof of operating address
- Proof of registered address if different than operating address
- Signature verification of the authorised signatory of the entity

Part III - On-going Due Diligence (Monitoring of Transactions)

The Company shall undertake ongoing due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth. Since, the Company is a housing finance company and all our loans are tenure based with a fixed or variable instalment paid through electronic clearing system (ECS/NACH) mandate or post-dated cheques or other electronic mode of payments, our monitoring structure will be relevant to our nature of operations. While unusually large cash transactions will be rare, the Company will still pay special attention to all unusually large cash transactions relevant to its loan ticket sizes and if any unusual transaction/development comes to our knowledge relating to money laundering the same will be verified and notified as required.

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. High risk accounts shall be subjected to more intensified monitoring and hence will be reviewed at least once in six months. Low and Medium risk accounts will be reviewed once in a year and will be triggered to be flagged as High Risk based on the indicators pre-defined.

Appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring may be considered for ongoing due diligence.

14. Periodic Updation of KYC

The Company shall conduct periodic updation of KYC documents at least once in every 2 years for high-risk customers, once in every 8 years for medium risk customers and once in every 10 years for low-risk customers from the date of opening of the account / last KYC updation. In this manner, the Company shall follow a risk-based approach for periodic updation of KYC and ensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

For updation of KYC documents, the Company, shall ensure compliance with the following:

14.1 Periodic Updation of KYC for Individual Customers

a. **No change in KYC information:** If no change in the KYC information, a self-declaration from the customer in this regard shall be obtained. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc.
b. **Change in address:** In case of a change in address of the customer, a self-declaration of new address shall be obtained from the customer. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc. Thereafter, the Company shall get the declared address verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables or such other methods as may be deemed appropriate. Further, HomeFirst shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation/ periodic updation.

   Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

14.2 In addition to the above, the Company shall take the following measures:

a. KYC updation shall also be applicable when there is no change in customer information but the documents available with the Company are not as per the current CDD standards.
b. 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.
c. The customer's PAN details, if available with the Company, shall be verified from the database of the issuing authority at the time of periodic updation of KYC also.
d. In case of receipt of the updated KYC information/ documents, the Company shall provide an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, the Company shall ensure 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.

e. In order to ensure customer convenience, the facility of periodic updation of KYC is available at any branch or through any of the online/ digital/ electronic channels of the Company.
f. The Company, in order to comply with the PML Rules, shall bind its customers, through a loan agreement or any other relevant document, that, in case of any update in the KYC information/ documents submitted by the customer at the time of establishment of business relationship or last submitted, the customers shall be required to submit to the Company the update of such documents, within 30 days of the update to such documents.

Part VII - Enhanced Due Diligence Procedure

15. Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section include use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

16. Following EDD measures shall be undertaken by HomeFirst for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

a. In case the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding.
~~b.~~ In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
c. Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
d. The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
e. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
f. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

17. Accounts **of Politically Exposed Persons (PEPs)**

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

a. Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
b. The identity of the person shall have been verified before accepting the PEP as a customer;
c. The decision to open an account for a PEP is taken at a senior level, in accordance with the Customer Acceptance Policy;
d. All such accounts are subjected to enhanced monitoring on an on-going basis;
e. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval will be obtained to continue the business relationship;
f. The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
g. These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

18. Client **accounts opened by professional intermediaries:**

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

a. Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b. The Company shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c. The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.
d. All the beneficial owners shall be identified where funds held by the intermediaries are not comingled at the level of the company, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the company, the Company shall look for the beneficial owners.
e. The Company shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
f. The ultimate responsibility for knowing the customer lies with the Company.

CHAPTER – VIII: RECORD MANAGEMENT

19. Management of the Records relating to Identification of Customers and Transactions

To ensure compliance with the record management requirements prescribed under the PMLA and the PML Rules, the Company shall take the following steps:

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

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

20. Records pertaining to Non-Profit Organizations to be Maintained

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered,

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.

CHAPTER – IX: REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA

21.

a. The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.
b. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Company which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of the Company, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.
c. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not place any restriction on operations in loan accounts merely on the basis that an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level. Every 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 paragraph 4(b) of the Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.
d. The Company shall have adequate systems, processes and procedures, including through electronic means depending on the requirements of the business and as appropriate, to enable effective identification and reporting of suspicious transactions.
e. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put into use as a part of effective identification and reporting of suspicious transactions.

CHAPTER – X: REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS

COMMUNICATIONS FROM INTERNATIONAL AGENCIES

22. Unlawful Activities (Prevention) (UAPA) Act, 1967

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

The details of the two lists are as under:

a. The **"ISIL (Da'esh) &Al-Qaida Sanctions List",** established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida.
b. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban.

Further, the Company shall ensure compliance with obligations under Weapons of Mass Destruction (WMD), UNSCR 1718 Sanctions List of Designated Individuals and Entities and such other lists as may be notified by appropriate authorities.

CHAPTER – XI: OTHER INSTRUCTIONS

23. 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.

While considering the requests for data/information from Government and other agencies, the Company shall first 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 mutual dealing except in following circumstances:

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

24. CDD Procedure and sharing KYC Information with Central KYC Records Registry (CKYCR)

HomeFirst shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer in line with the Operational Guidelines issued by CERSAI. The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, for 'Individuals' (accounts opened after April 1, 2017), as per the KYC templates. Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/ update the KYC data pertaining to accounts of individual customers opened prior to the above-mentioned dates at the time of periodic updation, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever any additional or updated information is obtained from any customer, the Company shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of such customer in CKYCR. Upon updation of any records of the customer, CKYCR electronically intimates all regulated entities dealing with such customer regarding updation of his / her / its KYC record. Once the Company receives such update , the Company shall retrieve such updated KYC records from CKYCR and update the KYC record maintained by the Company. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

For the purpose of establishing an account-based relationship, updation/ periodic updation, the Company shall seek from the customer KYC Identifier, or retrieve the KYC Identifier, if available from the CKYCR and proceed to obtain KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

a. there is a change in the information of the customer as existing in the records of CKYCR.
b. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms.

c. HomeFirst considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
d. the validity period of documents downloaded from CKYCR has lapsed.

25. Operation of Bank Accounts & Money Mules:

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." The Company shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND.

The Company shall allot UCIC while entering into new relationships with individual customers as also the existing individual customers.

26. Money Laundering and Terrorist Financing Risk Assessment

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

a. The Company does not operate in other countries or geographies;
b. The Company does not source or originate loans from other countries or geographies;
c. The Company extends loans to identified borrowers for which KYC due diligence has been put in place;
d. The Company verifies the end use of the loan;
e. The Company does not offer banking, liabilities, and term deposits; and
f. The Company offers loans or credit facilities with defined end-use
g. The loan disbursements made by the Company are either through electronic bank transfer or through DD. The Company collects the instalments (EMIs) from customers through NACH/ECS. All pre-closures and part payments made by the customers are accepted only by way of cheques/electronic mode/DD.

However, the Company will carry out "Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise annually to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk to which the Company may be exposed to. Such internal risk assessment shall be commensurate to its size, geographical presence, the complexity of activities/structure, etc.

The exercise undertaken by the Company shall be properly documented, and the assessment process will consider various relevant risk factors and will take cognizance of overall sector specific vulnerabilities, if any, that the regulator/supervisor may share.

The outcome of the exercise shall be put up to the Risk Management Committee and should be available to competent authorities and self-regulating bodies.

27. Introduction of New Technologies

The Company, for customer due diligence and on-going due diligence, shall evaluate and adopt appropriate new technologies including artificial intelligence and machine learning which shall be commensurate to the money laundering risk perceived for the business undertaken by the Company with its customers.

The Company shall identify and assess the ML/ TF risks that may arise with respect to new products, new business practices and the use of new or developing technologies for both new and pre-existing products,to the extent relevant to the Company as an HFC. In this regard, 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.

28. Quoting of PAN

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

29. Hiring of Employees and Employee Training

Recruitment: Adequate screening mechanism shall be in place as an integral part of their personnel recruitment/hiring process., including Know Your Employee / Staff Policy.

Training

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

30. Period for presenting payment instruments

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

31. Review of Policy

The Policy shall be reviewed annually by the Board of Directors. Any amendment to the Policy that is considered necessary for effective implementation of the KYC Program any time during the year shall be carried out by the Designated Director and shall be placed for ratification at the next meeting of the Board.

XXX