Manappuram Home Finance Limited
"Know your Customer (KYC)" and "Anti money laundering (AML)" POLICY

Approval Date : **23-Dec-2014**

Effective Date : **23-Dec-2014**

Last review Date : **29-Oct-2026**

Next Review Date : **Oct 2027**

Policy Owner : **Credit & Operations**

Approved By : **Board**

Version Control		
Version Number	Description	Date
Version 1	Framed	23-12-2014
Version 2	Modified	06-08-2018
Version 3	Modified	02-11-2018
Version 4	Modified	07-05-2019
Version 5	Modified	09-08-2019
Version 6	Modified	30-10-2019
Version 7	Modified	24-01-2020
Version 8	Modified	09-05-2020
Version 9	Modified	21-01-2021
Version 10	Modified	24-05-2021
Version 11	Modified	07-08-2021
Version 12	Renewal	01-02-2023
Version 13	Modified	08-08-2023
Version 14	Modified	08-11-2023
Version 15	Renewal	10-08-2024
Version 16	Modified	04-02-2025
Version 17	Modified	31-07-2025
Version 18	Modified	24-10-2025
Version 19	Modified	22-01-2026
Version 20	Modified	29-10-2026

Contents

I. Introduction 3

II. Objectives 3

III. Key Elements 4

IV. Definition of a Customer under the KYC Policy 4

V. KYC Policy 5

VI. Updation /Periodic updation 31

VII. Central know your customer registry 34

VIII. Record Management 34

IX. Reporting requirement under foreign account tax compliance act (FATCA) and common reporting standards (CRS) 36

X. Secrecy obligations and sharing of information 36

XI. CDD Procedure and Sharing kyc information with central kyc records registry (CKYCR) 37

XII. Requirements/obligations under international agreements communications from international agencies 39

XIII. Money laundering and terrorist financing risk assessment: 40

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

XIV Review, Modifications: 42

Annexure I- Customer Identification Procedure features to be verified and documents that may be obtained from customers 43

Annexure II- Beneficial Owner (BO) 49

Annexure III- List of suspicious transactions pertaining to housing loans: 51

Annexure IV- Declaration for Submitting Aadhar Pradhan Mantri Awas Yojana (Urban) 53

Annex V- Digital KYC Process 54

Annexure-VI- Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005): 70

Annexure-VII- Updation/ Periodic Updation of KYC– Revised Instructions 72

I.Introduction

1.1 National Housing Bank (NHB) has issued guidelines on Know Your Customer (KYC) and Anti-Money Laundering (AML) vide its circular bearing NHB/ND/DRS/POL – No. 33/2010-11 dated October 11, 2010 and NHB (ND)/DRS/ Policy Circular No 94 /2018-19 dated March 11, 2019 advising Housing Finance Companies (HFCs) to ensure that a proper policy framework on 'Know Your Customer' and 'Anti-Money Laundering Measures' is to be put in place and to follow certain customer identification processes for opening of accounts and monitoring transactions of suspicious nature keeping in view the possibility of the use of money through these accounts for criminal and other unlawful purposes for which a new legislation namely "Prevention of Money Laundering Act, 2002" has been framed. Also, RBI has issued the guidelines "Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025" dated 28th November 2025 updated as on 29th December 2025. The policy has been amended in line with the above circulars.

1.2 Manappuram Home Finance Limited (MAHOFIN) has framed its KYC & AML policy keeping in view the broad guidelines circulated by RBI/NHB in this regard.

1.3 Frequently Asked Questions (FAQs) on KYC can be accessed through the website "rbi.org.in" >> More links >> FAQs.

II. Objectives

2.1 The main objective of the KYC & AML policy of MAHOFIN is to ensure that its money is not used, intentionally or unintentionally, directly or indirectly, for any unlawful and prohibited activities or purpose particularly those which are covered by Prevention of Money Laundering Act, (PMLA) 2002 and keep the records by Prevention of Money-Laundering (Maintenance of Records)

Rules, 2005. At the same time KYC & AML Policy will also enable MAHOFIN to have more transparent and specific information about the customers and understand their financial dealings better. This in turn will enable MAHOFIN to effectively determine risk level involved in different Loan transactions and will help it to undertake effective risk management.

2.2 KYC & AML Policy shall be applicable to all types of customers including individual, partnership firms, employees, corporate entities, associates, trusts, societies or any other entity having a legal status. This policy will also cover those persons who are the real beneficiaries of the credit facilities extended by MAHOFIN and those who represent such persons or entities.

2.3 The Company shall report the Detection of the Currency Counterfeit Note to National Housing Bank, in the format, prescribed in the Circular NHB / ND / DRS / Misc. Circular No 19 / 2018-19 dated August 13, 2018.

III. Key Elements

As per the guideline issued by RBI/NHB, MAHOFIN has for formulated its KYC Policy based on the following four key elements:

(i) Customer Acceptance Policy (CAP);

(ii) Customer Identification Procedures (CIP);

(iii) Monitoring of Transactions and Maintenance of records of transactions and;

(iv) Risk Management.

IV. Definition of a Customer under the KYC Policy

4.1 For the purpose of KYC Policy, a 'Customer' will be defined as:

(i) A person or entity that maintains an account and/or has a business relationship with MAHOFIN,

(ii) One on whose behalf the account is maintained (i.e. the beneficial owner-Refer Annexure II),

(iii) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc. as permitted under the law, and

(iv) Any person or entity connected with a financial transaction which can pose significant reputational or other risks to MAHOFIN say a wire transfer or issue of a high value demand draft as a single transaction.

4.2 Besides KYC guidelines shall also be applicable to the following associates / agencies /intermediaries associated with MAHOFIN :

(i) Empanelled lawyers

(ii) Empanelled valuers

(iii) Vendors providing services like Selling Agents, Direct selling team, Collection Agencies, Field Investigation Agencies etc.

(iv) Builders

(v) Seller of property being financed by MAHOFIN

(vi) Any other intermediary

V. KYC Policy

In the formulation of this policy, as suggested by RBI/NHB's KYC guidelines, MAHOFIN has ensured that the adoption of customer acceptance policy and its implementation does not become too restrictive and must not result in denial of housing finance services to general public, especially to those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

5.1 Customer Acceptance Policy (CAP)

The following norms and procedures will be followed by MAHOFIN in relation to its customers who approach for availing Loan facilities. Also while taking decision to grant any one or more credit facility to customers as well as during the continuation or pre-closing of any loan account of the customer, the following norms will be adhered to by MAHOFIN:-

(i) No account opened will be in anonymous or fictitious / benami name(s); MAHOFIN shall insist for sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application;

(ii) Risk in terms of the location of customer and his clients and mode of payments are duly checked;

- Volume of turnover, social and financial status, etc. will form the basis for categorization of customers into low, medium and high risk.

- Customers requiring very high level of monitoring, e.g. Politically Exposed Persons will be given due consideration.

(iii) Documentation requirements and other information will be collected in respect of different categories of customers depending on perceived risk and guidelines issued from time to time; Declaration will be taken from the customer that the proceedings / transactions are not in violation of the PML Act, 2002 and RBI/NHB regulations in this regard.

(iv) Not to open an account or close an existing account where MAHOFIN is unable to apply appropriate customer due diligence measures, i.e. MAHOFIN is unable to verify the identify and / or obtain documents required as per the risk categorisation due to non co-operation of the

customer or non reliability of the data / information furnished to MAHOFIN. However, decision not to open or close an account shall be taken at a higher level after giving due notice to the customer explaining the reasons for such a decision to avoid harassment.

(v) All such loan requests where the customer, without sufficient cause, does not provide information and documentary evidence in terms of the requirements outlined by MAHOFIN in loan application form, to the satisfaction of MAHOFIN will not be processed unless the customer has genuine difficulty or reasons for not providing such information, but MAHOFIN even in the absence of the such information is otherwise satisfied about the identity and credentials of the customer on the basis of independent verification conducted by MAHOFIN at its own level without the knowledge of the customer.

(vi) While collecting information from the customers about his identity, work place, status, financial resources, it shall be kept in mind the obligations of MAHOFIN as Housing Finance MAHOFIN laid down under PMLA and Rules or Regulations framed there under, directions issued by RBI/NHB or any other Government agency on the matters relating to maintenance and furnishing of information by financial institutions to the authorities constituted under PMLA or any other authorities empowered under law to seek any information from MAHOFIN about the customers.

(vii) Permanent Address proof from new applicants will be collected. The documents which can be accepted as proof of address are mentioned in Annexure-I.

(viii) For existing customers who wish to pre-close their loan account with MAHOFIN following will be collected:

(a) Officially Valid Document (As per Annexure I)

(b) A declaration from the customer regarding source of funds being used for pre-closure of the loan account.

(c) Closure of the loan account authority will be restricted to authorized person only.

(ix) In the following circumstances, the account may be operated by a mandate holder or the account may be opened by an intermediary in a fiduciary capacity hence the customer is permitted to act on behalf of another person/entity, in conformity with the established law and practices:

(a) If applicant is NRI/PIO

(b) If applicant is a limited Company

(c) If applicant is a partnership firm

(x) Any other circumstance where it is not possible for the applicant to be present at the branch location physically available. Necessary checks before any loan disbursement will be carried out through Field Investigation Agency so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc

(xi) A Unique Customer Identification Code (UCIC) shall be allotted to the Customers. MAHOFIN shall apply the CDD procedure at the UCIC level

(xii) Additional information may be obtained which are not specifically mentioned in this policy with the explicit consent of the Customer.

(xiii) MAHOFIN need to ensure that the identity of the Customer does not match with the any person or entity whose name appears in the sanction lists.

(xiv) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by the company. If an existing KYC complaint customer desires to open another account or avail any other product or service, there shall be no need for a fresh CDD exercise as far as the identification of the customer is concerned.

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

(xvi) Where MAHOFIN is suspicious 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.

(xvii) 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.

(xviii) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated from time to time.

5.2 MAHOFIN will prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy and as per credit risk policy. The customer profile will contain information relating to the customer's identity, social/ financial status, nature of business activity, information about his clients' business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex 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. The nature and extent of due diligence will depend on the risk perceived by MAHOFIN. At the time of credit appraisal of the applicant the details are recorded along with his profile based on meeting with the applicant apart from collection of applicable documents; this shall be

as per our credit and product norms which will be incorporated in the operation manual. However, while preparing customer profile, MAHOFIN will seek only such information from the customer which is relevant to the risk category and is not intrusive and will be in conformity with the guideline. Further information if required from the customers will be sought separately with his/her consent after opening the account.

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

The risk level categorisation will be determined by considering the following information submitted by the customer:-

a) Nature of business of the customer
b) Workplace of customer and his clients
c) Volume of business six monthly/annual turnover
d) Social and financial status
e) Quantum and tenure of loan facility applied and proposed schedule for repayment of loan.

As per KYC policy, for acceptance and identification, customers are categorized broadly into low risk, medium risk, and high risk categories:-

(i) ***Low Risk Customers*** for the purpose of this policy will be individuals and entities whose identities and sources of wealth can be easily identified, have structured income and transactions in whose accounts by and large conform to the known profile. Illustrative examples of low risk customers could be:
   (a) Salaried applicants with salary paid by cheque.
   (b) People belonging to government departments.

(c) People working with government owned companies, regulators and statutory bodies etc.

(d) People belonging to lower economic strata of the society whose accounts show small balances and low turnover.

(e) People working with Public Sector Units

(f) People working with reputed Public Limited companies & Multinational Companies.

(ii) ***Medium Risk Customers*** would include:

(a) Salaried applicants with variable income/unstructured income, receiving salary in cheque.

(b) Salaried applicants working with Private Limited Companies.

(c) Self Employed professionals other than HNIs

(d) Self Employed customers with sound business and profitable track record for a reasonable period.

(e) High Net worth Individuals-with occupational track record of more than 3 years.

(iii) ***High Risk Customers*** that are likely to pose a higher than average risk to MAHOFIN may be categorized high risk customers depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. MAHOFIN will examine the case in detail based on the risk assessment as per MAHOFIN's credit risk policy and guidelines of Credit Policy. Examples of high risk customers requiring higher due diligence may include:

(a) Non-resident customers,

(b) High net worth individuals, without an occupational track record of more than 3 years.

(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) Non-face to face customers

(h) Those with dubious reputation as per available public information etc.

The risk categorisation of the 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.

MAHOFIN's exposure to any of the clients is subject to its credit risk policy and Credit Policy. However, for customer acceptance, KYC is a prerequisite for a credit risk grading.

5.4 Customer Identification Procedure (CIP)

5.4.1 Customer Identification means identifying the customer and verifying his/ her / its identity by using reliable, independent source of documents, data or information while establishing a relationship. MAHOFIN will obtain sufficient information such as Voter ID card, PAN number, Passport etc. necessary to establish, to its satisfaction the identity of each new customer, whether regular or occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected for the purpose of the intended nature of relationship.

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

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); **or**

(ii) he decides to submit his **Aadhaar number voluntarily** with declaration for submitting Aadhar (refer Annexure IV) to company notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or

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

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

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above, notified under first proviso to sub-section (1) of section 11A of the PML Act, Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Company.

ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Company shall carry out offline verification.

iii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under **Annex V.**

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under **Annex V.**

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

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

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

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

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

Explanation 4: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer 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), the customer shall provide the Aadhaar number to the NBFC. In other cases, customers may provide the Aadhaar number voluntarily.

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

For customers that are legal persons or entities, MAHOFIN will:

(i) Verify the legal status of the legal person/ entity through proper and relevant documents.

(ii) Verify that any person purporting to act on behalf of the legal person/entity is so authorized. Also the identity of that person is verified and For (i) & (ii) Memorandum of Association and board resolution will be collected to

ensure that the person purporting to act on behalf of the legal person/entity is authorized to do so, apart from applicable field/document investigations. In case of partnership firm, a copy of partnership deed along with the registration certificate of the firm, if registered and power of attorney in favour of the person purporting to act on behalf of the firm shall be collected.

(iii) In order to authenticate the identity of the person so purporting to represent the company / Firm, Signature verification / attestation shall be done either from the Banker or notary, copy of passport, driving license or pan card to be taken of person who purporting to represent the company.

(iv) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. MAHOFIN will collect Shareholding letter duly certified by the company Secretary / Company's Auditor/Chartered accountant and Necessary Resolution / authorisation etc.

5.4.4 RBI, vide its circular no DOR.AML.BC.No.27/14.01.001/2019-20 dated January 09, 2020 and Gazette Notification G.S.R. 582(E) dated August 19, 2019 has permitted "Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

The brief procedure for conducting V-CIP is given below:

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

i. The official of the company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

• **Banks:** can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP.

• **Others:** can only carry out Offline Verification of Aadhaar for identification.

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

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

iv. The official of the Company shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the **customer undertaking** the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

vii. Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. The company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

Explanation: Making specific facial gestures, like blinking of eyes, smiling, frowning, etc. is not mandatory for liveness check. The Company will take due

cognizance of special needs, if any, of the customer during liveness check.

viii. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

ix. The audio-visual interaction shall be triggered from the domain of the Company itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.

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

xi. The company, are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Company.

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

The ultimate responsibility for customer due diligence will be with the Company.

5.4.5 Due diligence for High risk customer identification will be as follows:

(a) **Non-resident customers:** Due diligence including email verification of employment of the customer, collection of a local guarantor & power of attorney alongwith their identification proofs and verification of their residence/office will be done, if found necessary.

(b) **High net worth individuals:** With less than three years occupational

track record, due diligence including personal discussion with the applicant, analysis of bank statement and financial statements with be done, details of client profile, sources of fund will be obtained, if required.

(c) Trusts, Charities, NGOs and organizations receiving donations: As and when such cases are received due diligence to be undertaken as for other cases in the high-risk categories.

(d) Companies having close family shareholding or beneficial ownership: Due diligence including personal discussion with the applicant will be done. In case of company's proportionate income being considered to the extent of the customer's Shareholding in the Company – board resolution authorising the director(s) to sign on behalf of the company will be collected. Also, signature verification of the person(s) issuing the board resolution will be collected, if necessary.

(e) Firms with 'Sleeping partners': Due diligence including personal discussion with the applicant will be done. If income of the partnership firm is being considered, then MAHOFIN will collect a letter signed by all the partners authorising the concerned partner(s) to sign on behalf of the partnership to be continued. Also signature verification of the person(s) issuing this authority letter will be collected, if necessary.

(f) **Politically exposed persons (PEPs) of foreign origin:** Same due diligence as NRI/PIO to be undertaken.

A. The Company shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

(a) MAHOFIN have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

(b) Reasonable measures are taken by the company for establishing the source of funds / wealth;

(c) Approval to open an account for a PEP shall be obtained from the senior management; sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

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

(g) Non-face to face customers: Due diligence including telephone/personal discussions be done, if required. Information from reliable sources will be obtained for establishing the existence of the person.

(h) Customer with dubious reputation: If found dubious then the case will not be entertained.

5.4.6 On-going Due Diligence

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. *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.

C. Simplified Due Diligence

Simplified norms for Self Help Groups (SHGs)

a. CDD of all the members of SHG shall not be required while opening the account of the SHG.
b. CDD of all the office bearers shall suffice.
c. Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

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

(a) Trust Nominee or Fiduciary Accounts :

There exists the possibility that a trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Hence, as and when such cases are received, MAHOFIN will determine whether the customer is acting on behalf of another person as trustee/ nominee or any other intermediary. If so, MAHOFIN may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, may also obtain details of the nature of the trust or other arrangements

in place. In the case of a 'foundation', steps will be taken to verify the founder managers/directors and the beneficiaries, if defined.

(b) Accounts of companies and firms

MAHOFIN will be careful while processing the cases of business entities specially to establish that individuals are not using those entities for maintaining accounts with it. MAHOFIN shall seek information, if required, on the control structure of the entity, source of funds and the natural persons who carry a controlling interest in the management.

These requirements may be moderated as per MAHOFIN's credit risk policy and guidelines of the Credit Policy, for e.g. in the case of a public company it will not be necessary to identify all the shareholders.

(c) Client accounts opened by professional intermediaries

When MAHOFIN has knowledge or reason to believe that the client account opened by a professional intermediary like Direct Selling Agent or Direct selling team or any other sales intermediary by whatever name called is on behalf of a single client, that client will be identified. Where MAHOFIN relies on the 'customer due diligence' (CDD) done by an intermediary like Field investigation agency or technical agency or lawyer or any other operation processing intermediary by whatever name called, MAHOFIN will ensure that the intermediary is having a bonafide identity with an established track record.

(d) Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, including the Head of States /Governments, senior politicians, senior government or judicial or military officers, senior executives of state-

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

(e) Accounts of non-face-to face customers:

In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, MAHOFIN will do telephone/personal discussion with the applicant, if necessary. Applicant will be met by the Sales representative of MAHOFIN and will fill up the meeting sheet on that basis to mitigate the higher risk involved, as applicable. Certification of all the documents presented will be insisted upon and, if necessary, additional documents may be called for and applicable verification of these documents will be done. Hence apart from the existing due diligence for such customers MAHOFIN shall take resident Indian Co-applicant as a party to the loan proposal or a local resident guarantor to the loan with identity verification.

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

5.4.8 MONITORING OF TRANSACTIONS

(a) Ongoing monitoring is an essential element of effective KYC procedures. Since MAHOFIN is a housing finance company and all its loans are tenure based with a fixed/ variable instalment paid through Electronic Clearing System (ECS) mandate or post dated cheques, the monitoring structure will be relevant to the nature of operations.

MAHOFIN will pay special attention to all unusually large transactions involving large cash. MAHOFIN shall introduce cash transaction reporting system above Rupees Ten Lacs. Risk categorization as is mentioned in this policy may be updated as and when required by the management. In case of overdue/default accounts where there is scope for meeting or vetting the profile of this customer again, due diligence if found necessary will be carried out. Subsequent to MAHOFIN's sanction, during the period of part disbursement till full disbursement if any unusual transaction/ development comes to MAHOFIN's knowledge relating to money laundering the same will be verified and notified as required, MAHOFIN will ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML, Act, 2002. MAHOFIN will ensure that transactions of suspicious nature as defined in Annexure III and/or any other type of transaction notified under section 12 of the PML, Act, 2002, is reported to the appropriate law enforcement authority, as and when detected by our officials through the Principal Officer.

(b) MAHOFIN will maintain proper record in accordance with the PML, Act, 2002, of all cash transactions (deposits and withdrawals) of Rupees Ten Lacs and above. As a matter of policy, MAHOFIN shall not accept deposits in cash over Rupees two Lakhs. No loan is disbursed in cash and no monthly instalment above Rupees two Lakhs is accepted in cash. Any transactions of suspicious nature as per Annexure III are to be reported to the Principal Officer immediately. In addition thereto, the Branches shall on monthly basis furnish a certificate to the Principal Officer evidencing that neither such prohibited transactions and/nor cash transaction as specified in the policy have taken place.

5.4.9 RISK MANAGEMENT

(a) Internal Audit :

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

(b) Hiring of Employees and Employee Training:

MAHOFIN will have an ongoing employee training program so that the members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

(a) The Company shall put in place mechanism as an integral part of their personnel recruitment/hiring process for adequate screening.

(b) MAHOFIN 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. MAHOFIN shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in 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 RE, regulation and related issues shall be ensured.

(c) Customer Education:

MAHOFIN will educate the customer on the objectives of the KYC programme so that customer understands and appreciates the motive and purpose of collecting such information.

(d) Introduction of New Technologies:

MAHOFIN 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, MAHOFIN 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.

(e) KYC for the Existing Accounts:

MAHOFIN will apply the KYC norms to the existing customers of loan accounts on the basis of materiality and risk envisaged by it for those existing loan accounts.

(f) Non-Cooperation by the customer in respect of KYC norms:

Where MAHOFIN is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer for KYC compliance, MAHOFIN will follow up with the existing identified customer for KYC Compliance. Closure decision if at all is required will depend upon MAHOFIN's internal assessment and will be taken at a

Senior Level of Zonal Heads/GM and above only after issuing due notice to the customer explaining the reasons for taking such a decision.

(g) Applicability to branches and subsidiaries outside India

This will not be applicable to MAHOFIN as it has no branches or subsidiary outside India, whenever MAHOFIN takes any decision in this respect, it will formulate appropriate KYC policy for these branches/subsidiaries.

(h) Appointment of Designated Director

Chairman of the Board has been appointed as 'Designated Director' to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.

(i) Appointment of Principal Officer:

MAHOFIN has designated Company Secretary, as 'Principal Officer'. Principal Officer is stationed at Head-Office and will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. She will maintain close liaison with enforcement agencies. She will also ensure that there is proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines. However, any such action will be documented and placed before the management committee of MAHOFIN. Principal Officer will also report any unusual matter/information to the management committee of MAHOFIN as and when it occurs.

(j) Senior Management for the purpose of KYC complinace

Senior Management for the purpose of KYC compliance shall mean Heads of each department in the Company**.** The Senior Management shall assist the Principal Officer/Designated Director in the effective implementation of this policy.

(k) Maintenance of Records of Transactions (As per Rule 3 of the Prevention of Money Laundering Rules 2005):

MAHOFIN will maintain proper record of the under mentioned transactions:

(i) All cash transactions of the value of more than rupees Ten Lacs or its equivalent in foreign currency, though by policy MAHOFIN do not accept cash deposits in foreign currency.

(ii) All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lacs or its equivalent in foreign currency where such series of transactions have taken place within a month.

(iii) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions.

(iv) All suspicious transactions as mentioned in Annexure III**.**

(l) Information to be preserved:

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

(a) The nature of the transactions

(b) The amount of transactions and currency in which it was denominated

(c) The date on which the transaction was conducted and

(d) Parties to the transactions

(m) The sanctions and disbursements are done on the system; hence it has a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required. However, MAHOFIN will maintain account information for at least ten years from the date of cessation of transaction between MAHOFIN and the client, all necessary records of transactions, which will make available individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

MAHOFIN will ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. Apart from this, the application form, copy of loan agreement, NOC, other document either photocopy or cancelled original copy will be kept for next ten years after the full closure of the account. However, preservation and maintenance of the documents will be in paper form and a soft copy.

The identification of records and transaction data will be made available to the competent authorities upon request only through the principal officer under this policy with his approval.

(n) Reporting to Financial Intelligence Unit – India

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

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

The Company shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

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 of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list to ensure compliance with the Order dated September 1 , 2023, titled - "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)", issued by the Ministry of Finance, Government of India, In case of match in the above cases, Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO) (FIU-Ind). A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. The Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems has been attached mentioned in Annexure VI.

(o) Compliance under Foreign Capital Contribution (Regulation) Act, 1976

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

(p) Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

Company shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, company shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

VI. Updation /Periodic updation

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

In respect of an individual customer who is categorized as low risk, the Company shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The Company shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due. The revised instructions on Updation/Periodic updation are provided in Annexure-VII.

a) For 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 MAHOFIN, Customer's mobile number registered with the MAHOFIN, digital channel (such as mobile application), 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 MAHOFIN, Customer's mobile number registered with the MAHOFIN, digital channel (such as mobile application), 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, MAHOFIN, may at its option, obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as mentioned in Annexure I, for the purpose of proof of address, declared by the Customer at the time of updation/periodic updation.

iii. MAHOFIN is not using the services of Business Correspondent (BC) for Updation/ Periodic Updation of KYC.

b) Customers Other than Individuals:

i) No change in KYC information: In case of no change in the KYC information of the LE Customer, a self-declaration in this regard shall be obtained from the LE Customer through its email id registered with MAHOFIN, digital channels (such as mobile application), letter from an official authorized by the LE in this regard, board resolution etc. Further, MAHOFIN shall during this process ensure that the Beneficial Ownership (BO) information available 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, MAHOFIN shall undertake the KYC process equivalent to that applicable for on-boarding a new LE Customer.

c) **Additional Measures:** In addition to the above, MAHOFIN shall also ensure that,

i) The KYC documents of the Customer as per the current CDD standards

is available at all times. Further, in case the validity of the CDD documents available with MAHOFIN has expired at the time of periodic updation of KYC, MAHOFIN shall undertake the KYC process equivalent to that applicable for on-boarding a new Customer.

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

iii) An 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 updation/periodic updation. The Company shall ensure that the information /documents obtained from the Customers at the time of updation/periodic updation of KYC are promptly updated in the records/database and an intimation mentioning the date of updation of KYC details to be provided to Customer.

iv) In order to ensure Customer convenience, MAHOFIN may consider making available the facility of periodic updation of KYC at any of its branches.

v) MAHOFIN shall adopt a risk-based approach with respect to periodic updation of KYC.

vi) MAHOFIN shall advise the customers that 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; MAHOFIN will collect the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at MAHOFIN's end.

vii) The MAHOFIN shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, MAHOFIN shall give at least three advance intimations, including at least one intimation by

letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, MAHOFIN shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. MAHOFIN shall intimate/ remind the Customers via letter which may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded in the Company's system against each customer for audit trail.

VII. Central know your customer registry

The Company shall upload the Know Your Customer (KYC) data with CERSAI in respect of new individual accounts opened on or after the date of NHB Circular NHB (ND) / DRS / Policy Circular No. 76 /2016-17 dated November 1, 2016. Company shall capture the KYC information for sharing with the Central KYC Record Registry in the manner mentioned in the "Prevention of Money – Laundering (Maintenance of Records) Rules, 2005" (and amendments thereto), as required by the revised KYC templates prepared for individuals and non - Individuals / legal entities, as the case may be

VIII. Record Management

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

The Company shall:

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

(b) preserve the records pertaining to the identification of the customers and their

addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

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

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

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

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv)the parties to the transaction.

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

(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation. – For the purpose of this Section, 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

MAHOFIN 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, MAHOFIN shall register the details on the DARPAN Portal. MAHOFIN shall also maintain such registration records for a period of five years after the business relationship between the customer and the MAHOFIN has ended or the

account has been closed, whichever is later.

IX. Reporting requirement under foreign account tax compliance act (FATCA) and common reporting standards (CRS)

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

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

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

X. Secrecy obligations and sharing of information

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between MAHOFIN and customer.

(b) 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.

(c) While considering the requests for data/information from Government and other agencies, company 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.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of MAHOFIN requires disclosure and

iv. Where the disclosure is made with the express or implied consent of the customer.

XI. CDD Procedure and Sharing kyc information with central kyc records registry (CKYCR)

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. The Company shall upload the KYC data pertaining to all new individual accounts with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

The Company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual/LE as the case may be.

The Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs at the time of periodic updation as specified in this policy, when the updated KYC information is obtained/received from the customer. Also, whenever the Company obtains additional or updated information from any customer as per below paragraph or Rule 9 (1C) of the PML Rules, 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 the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the 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 or for verification of identity of a customer, the Company shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

(i) there is a change in the information of the customer as existing in the records of CKYCR; or

(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or

(iii) the validity period of downloaded documents has lapsed; or

(iv) the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

Explanation: The Regulated Entity that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, the Company downloading and relying on such records from the CKCYR shall not be required to re-verify the authenticity of the customer's identity and /or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. The Company downloading and relying on KYC records downloaded from the CKCYR shall remain responsible for all aspects of CDD procedure and provisions of these Directions, except verification of identity and / or address of the customer.

XII. Requirements/obligations under international agreements communications from international agencies

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 and amended 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", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

(b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/3ppp1en-taliban.htm

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

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

The procedure laid down in the UAPA Order dated February 2, 2021 (Annex VI) shall be strictly followed and meticulous compliance. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)- The Company shall update the list as notified by RBI from time to time.

The Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

In addition to the above, The Company shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act

Latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements to be leveraged.

Company shall undertake counter measures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

XIII. Money laundering and terrorist financing risk assessment:

Under the RBI regulation issued vide circular reference no DOR.AML.BC.No.66/14.01.001/2019-20 dated April 20 2020 regarding the Internal ML/TF risk assessment the following shall be adopted:

(a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the company shall take cognizance of the overall sector-specific vulnerabilities, if any, shared by the regulator / supervisor from time to time.

(b) The risk assessment shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. Further, the periodicity of risk assessment exercise shall be determined by the Board, in line with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

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

d. **Wire transfer** refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

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

FATF Statements circulated by Reserve Bank of India from time to time, and publicly

available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. The Company shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

XIV Review, Modifications:

This policy shall be reviewed on a yearly basis. However, depending on requirement, the review may be done at shorter intervals. Any changes in the policy shall be with approval of Board.

Annexure I- Customer Identification Procedure features to be verified and documents that may be obtained from customers

Features	Documents (Certified Copy)
Individuals Legal name and any other names used	(i) Pan card OR Form 97 "Officially Valid Documents" **i) Passport** ii) Voter's Identity Card iii) Driving **License** iv) NREGA Job Card v) letter issued by the National Population Register vi) proof of possession of Aadhaar number
Sole Proprietary	(i) Pan card OR Form 97 "Officially Valid Documents" i) Passport ii) Voter's Identity Card iii) Driving License iv) NREGA Job Card v) letter issued by the National Population Register vi) proof of possession of Aadhaar number Any two documents as a proof of business/ activity in the name of the proprietary firm (Mandatory) (a) Registration certificate including Udyam Registration Certificate (URC) issued by the Goverment (b) Certificate/license issued by 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/ Licence/certificate (g) Complete Income Tax Return (not just the acknowledgement) duly authenticated/acknowledged by the Income Tax authorities. (h) Utility bills such as electricity, water, and landline telephone bills.
Companies	**Certified Copies of each of the following:** (a) Certificate of incorporation. (b) PAN Card of the Company (c) Memorandum and Articles of Association. (d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf. (e) Identification information as defined for individual in respect of managers, officers or employees holding an attorney to transact on its behalf. (f) the names of the relevant persons holding senior management position; and (g) the registered office and the principal place of its business, if it is different.
Partnership Firms	**Certified Copies of each of the following:** (a) Registration certificate. (b) Partnership deed. (c) Identification information as defined

	for individual in respect of the person holding an attorney to transact on its behalf (d) PAN Card of the Partnership firm (e) The names of all the partners and (f) address of the registered office, and the principal place of its business, if it is different.
Trusts - Names of trustees, settlers, beneficiaries and signatories. - Names and addresses of the founder the managers/directors and the Beneficiaries telephone/fax numbers	**Certified Copies of each of the following:** (a) Registration certificate. (b) Trust deed. (c) Identification information as defined for individual in respect of the person holding a power of attorney to transact on its behalf. (d) Permanent Account Number or Form No.60 of the trust (e) the names of the beneficiaries, trustees, settlor and authors of the trust f) the address of the registered office of the trust; and (g) list of trustees and documents as are required for individuals for discharging the role as trustee and authorised to transact on behalf of the trust
Unincorporated Association or a Body of Individuals	**Certified Copies of each of the following:** (a) resolution of the managing body of such association or body of individuals; (b) power of attorney granted to transact on its behalf; (c) Identification information as defined for individuals in respect of the person holding an attorney to transact on its behalf and (d) such information as may be required by MAHOFIN to collectively establish the

	legal existence of such an association or body of individuals (e) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
Juridical Persons (Government or its Departments, societies, universities and local bodies like village panchayats)	**Certified Copies of each of the following to be obtained and verified:** (a) Document showing name of the person authorised to act on behalf of the entity; (b) Aadhaar/ PAN/ Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and (c) Such documents as may be required by MAHOFIN to establish the legal existence of such an entity/juridical person.

***Note**:*

1. ***Unregistered trusts/partnership firms shall be included under the term unincorporated association'.***
2. ***Explanation: Term 'body of individuals' includes societies***

a. "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, letter issued by the National Population Register containing details of name and address.

a. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereofshall be deemed to be OVDs for the limited purpose of proof of address:-

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings,if they contain the address;
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

b. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'a' above
c. where the OVD presented by a foreign national does not contain the detailsof 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.

B .Government of India, vide Gazette Notification G.S.R. 381(E) dated May 28, 2019, has notified following amendment to the Prevention of Money-laundering (Maintenance of Records) Rules, 2005:

"Where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail."

c. Aadhaar based e-KYC through OTP / Biometric Authentication

In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, UIDAI has launched its e-KYC service. The Company shall accept

e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an officially valid document under PML Rules.

The Company may provide an option to the customer for e-KYC through Aadhaar based One Time Pin (OTP). Accounts opened in terms of this proviso i.e., using Aadhaar based OTP, are subject to certain conditions as stipulated in the NHB Circular NHB (ND)/DRS/Policy Circular No.85/2017-18 dated December 08, 2017 and NHB(ND)/DRS/REG/MC-04/2018 July 02, 2018.

Further, to ease out the process of biometric authentication for e-KYC verification performed at the branches/offices of the HFC, KYC verification, through Aadhaar based biometric authentication, may be performed by the Authorised Person of the Company also and shall be accepted as a valid process for KYC verification subject to the conditions as stipulated in the referred Circular.

Physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post and e-KYC process mentioned in the circular NHB (ND) / DRS / Policy Circular No.72 / 2014-15 dated April 23, 2015.

d. “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.

Annexure II- Beneficial Owner (BO)

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

Note- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 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 incorporated association or body of individuals.

Note: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

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

Identification of Beneficial Owner

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

(a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

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

Annexure III- List of suspicious transactions pertaining to housing loans:

a) Customer is reluctant to provide information, data, documents;
b) Submission of false documents, data, purpose of loan, details of accounts;
c) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc;
d) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
e) Approaches a branch/office of 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;
f) Unable to explain or satisfy the numerous transfers in the statement of account/multiple accounts;
g) Initial contribution made through unrelated third-party accounts without proper justification;
h) Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
i) Suggesting dubious means for the sanction of loan;
j) Where transactions do not make economic sense;
k) There are reasonable doubts over the real beneficiary of the loan and the home to be purchased;
l) Encashment of loan amount by opening a fictitious bank account;
m) Applying for a loan knowing fully well that the property/dwelling unit to be financed has been funded earlier and that the same is outstanding;
n) Sale consideration stated in the agreement for sale is abnormally higher/ lower than what is prevailing in the area of purchase;
o) Multiple funding of the same property/dwelling unit;
p) Request for payment made in favour of a third party who has no relation to the transaction;

q) Usage of loan amount by the customer in connivance with the vendor/ builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated.

r) Multiple funding/financing involving NGO/Charitable Organization / Small/Medium Establishments (SMEs)/ Self Help Groups (SHGs)/ Micro Finance Groups (MFGs)

s) Frequent requests for change of address;

t) Overpayment of instalments with a request to refund the overpaid amount.

Annexure IV- Declaration for Submitting Aadhar Pradhan Mantri Awas Yojana (Urban)

Ministry of Housing and Urban Affairs, Government of India

Consent for Authentication

I. I hereby state that I have no objection in authenticating myself with Aadhaar based authentication system and consent to providing my Aadhaar number, Biometric and / or One-Time Password (OTP) data for Aadhaar based authentication for the purposes of availing benefits of owning a pucca house under Pradhan Mantri Awas Yojana (Urban) [PMAY(U)]. I understand that the Aadhaar number, Biometrics and/ or OTP I provide for authentication shall be used:-

a. for authenticating my identity and;

b. for de-duplication within verticals of PMAY(U) and other housing schemes like PMAY(Gramin), Rural Housing Interest Subsidy Scheme (RHISS).

II. I understand that PMAY (Urban), Ministry of Housing and Urban Affairs, Government of India shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication.

III. I hereby declare that the information provided hereunder is correct.

Name : _____

Masked Aadhaar Number : _____

Mobile Number : _____

Enclosure: Copy of the Aadhaar Id self-attested.

Signature of applicant

Date _____

(To be filled by ULBs/implementing Agencies/PLIs/HFCs)

Domain Id: _____

Registration No. (if any) _____

Annex V- Digital KYC Process

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

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

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

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

G. The live photograph of the customer and his original documents shall be captured in

proper light so that they are clearly readable and identifiable.

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

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

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

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

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

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

Annexure VI

Procedure for implementation of Section 51A of the UnlawfulActivities (Prevention) Act, 1967.

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) read as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —

a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged inor suspected to be engaged in terrorism;

b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

c) prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under: - "Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:

3. Appointment and communication details of the UAPA Nodal Officers :

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA **[Telephone Number: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].**

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to theCentral [designated] Nodal Officer for the UAPA.

3.3 All the States and UTs shall appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.4 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

3.5 The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies.

3.6 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.

4. Communication of the list of designated individuals/entities:

4.1 The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988 Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs

would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU–IND, CTCR Division and Foreigners Division in MHA.

4.2 The Financial Regulators shall forward the list of designated persons as mentioned in Para 4(i) above, without delay to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies.

4.3 The Central [designated] Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 4(i) above, to all the UAPA Nodal Officers of States/UTs without delay.

4.4 The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay.

4.5 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.

5. Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc.

5.1 The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by the SEBI and insurance companies requiring them -

(i) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in theSchedule to the Order, hereinafter, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held inthe form of bank accounts, stocks, Insurance policies etc., with them.

(ii) In case, the particulars of any of their customers match with the particulars of

(iii) designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

(iv) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in 5.1
(ii) above to the UAPA Nodal Officer of the State/UT where the account is held andto Regulators and FIU-IND, as the case may be, without delay.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No.011-23092551 and also convey over telephone No.011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI, and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.
On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/ entities identified by the banks, stock exchanges/depositories, intermediaries and

insurance companies are the ones listed as designated individuals/ entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

5.2 In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, so that any individual or entity may be prohibited frommaking any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The Central [designated] Nodal Officer for the UAPA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designatedindividual/entity.

6. Regarding financial assets or economic resources of the nature of immovable properties:

6.1 The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction, without delay.

6.2 In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.

6.3 The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.

6.4 The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

6.5 In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA NodalOfficer of the State/UT.

The order shall be issued without prior notice to the designated individual/entity.

6.6 Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources orrelated services available for the benefit of the individuals or entities listed in the

Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

7. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.

(ii) The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not carry out such transaction and without delay inform the CBIC, who in turn follow thesimilar procedure as laid down in the paragraphs 6.2 to 6.5 above.

(iii) The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organizations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, inturn, follow the procedure as laid down in the paragraphs 6.2 to 6.5 above. The Registrar should also be advised that no societies/ firms/ non-profit organizations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in

turn, follow the procedure laid down in the paragraphs 6.2 to 6.5 above.

(iv) The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraph 6.2 to 6.5 above

(v) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to sensitize their respective members to the provisions of Section 51A of UAPA, so that if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(vi) The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any of designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or abeneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in

paragraph 6.2 to 6.5 above.

(vii) In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(viii) The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms. Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

8. Regarding implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001:

8.1 The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities,

including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

8.2 To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

8.3 The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, onewho finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND andto the Nodal Officers of the States/UTs. The proposed designee, as mentionedabove would be treated as designated individuals/entities.

9. Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

10. Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.

10.1 The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:-

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds orother financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

(b) necessary for extraordinary expenses, provided that such determinationhas been notified by the MEA;

10.2. The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of:

(a) interest or other earnings due on those accounts, or

(b) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002),

Provided that any such interest, other earnings and payments continue to besubject to those provisions;

11. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person:

11.1 Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable

Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.

11.2 The banks, stock exchanges/depositories, intermediaries regulated bySEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

11.3 The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.

11.4 As regards prevention of entry into or transit through India of the designated individuals, the UAPA Nodal Officer in the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

11.5 The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in Foreigners Division of MHA.

12. Procedure for communication of compliance of action taken under Section 51A: The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in

the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

13. Regarding prevention of entry into or transit through India:

14. **Communication of the Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967:** The order issued under Section 51A of the Unlawful Activities (Prevention) Act, 1967 by the Central [designated] Nodal Officer for the UAPA relating to funds, financial assets or economic resources or related services, shall be communicated to all the UAPA nodal officers in the country, the Regulators of Financial Services, FIU-IND and DNFBPs, banks, depositories/stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties through the UAPA Nodal Officer of the State/UT.

15. The Company shall ensure strict compliance of this order.

Annexure-VI- Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

a) MAHOFIN shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India.

b) In accordance with paragraph 3 of the aforementioned Order, MAHOFIN ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

c) MAHOFIN shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

d) In case of match in the above cases, MAHOFIN will immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO),designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

e) MAHOFIN may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, MAHOFIN shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

g) In case an order to freeze assets under Section 12A is received by the MAHOFIN from the CNO, MAHOFIN will take necessary action to comply with the Order.

h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by MAHOFIN along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

Annexure-VII- Updation/ Periodic Updation of KYC– Revised Instructions

The revised instructions Updation/ Periodic Updation of KYC was issued by RBI via circular ref DOR.AML.REC.31/14.01.001/2025-26, dated June 12, 2025. The details are given below:

The customers' KYC Identifier shall be the first reference point for the purpose of establishing an account-based relationship or for verification of identity of customers. Accordingly, while onboarding customer, the Company shall download customers' KYC records online from CKYCR with customer's consent without requiring him/ her to submit the same records again, unless there is a change in records available with CKYCR.

The processes of onboarding customer and updation/ periodic updation of KYC have been simplified and the same are given below:

A. Face-to-face mode for onboarding the customer

(i) Customer may be onboarded in face-to-face mode through Aadhaar biometric based e-KYC authenticating and, in such case, if customer wants to provide a current address, different from the address as per the identity information available in the UIDAI database (i.e., Central Identities Data Repository), he may give a self-declaration to that effect to the Company.

(ii) Further, Digital KYC process is also allowed for customer onboarding.

B. **Non-face-to-face (NFTF) modes for onboarding the customer**

(i) Consent-based onboarding of customer in NFTF mode may be done using Aadhaar OTP based e-KYC authentication which is subject to certain conditions. Further, such account shall be placed under strict monitoring, and Customer Due Diligence (CDD) procedure shall be completed within a year.

(ii) Customer onboarding in NFTF mode using digital modes such as KYC Identifier, equivalent e-documents, documents issued through DigiLocker, and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs are subject to certain conditions.

C. Customer onboarding using Video based Customer Identification Process (V-CIP)

(i) V-CIP is an alternate method of CDD by an authorised official of the company by undertaking seamless, secure, live, informed and consent based audiovisual interaction with the customer to obtain identification information required for CDD purpose.

(ii) V-CIP is treated on par with face-to-face onboarding.

D. Simplified process of updation and periodic updation of KYC

(i) **Self-declarations** – The Company is allowed to obtain self-declaration regarding "*no change in KYC information*" or "*a change only in address details*" from customers using digital and non-digital modes, through customer's email / mobile number registered with the Company, digital channels (such as mobile application of the Company), letter, BCs, etc.

(ii) The updation/ periodic updation of KYC records are allowed to be carried out at any branch of the Company with which the customer maintains the account.

(iii) Aadhaar OTP based e-KYC and V-CIP are permitted for the purpose of updation/ periodic updation of KYC.

(iv) The Company has been directed to update customers' KYC information/ records based on the update notification received from CKYCR.