Know Your Customer & Anti-Money Laundering Policy

Recommended by

CEO

Date of Origination-6.8.2011

Date of subsequent Modifications: - 1.10.2013 ,11.11.2015,25.7.2017 , 10.5.2018 ,27.4.2019, 11.7.2020,8.2.21,30.04.2022 ,28.04.2023 ,19.6.2023 , 2.11.2023 , 6.11.2024 and 27.01.2025.

Vesrion-13.5

Approved by:

Board of Directors

Date of Approval:5.2.2025

INDEX

The National Housing Bank (NHB)/Reserve Bank of India (RBI) had advised all the HFCs to ensure that a proper policy framework on Know Your Customer and Anti Money Laundering measures is formulated and put in place with approval of the Board. The policy was to lay down the systems and procedures to help control financial frauds, identify money laundering and suspicious transactions, combating financing of terrorism and careful scrutiny/ monitoring of large value of cash transactions. Pursuant to advice from the NHB/RBI, a Know Your Customer and Anti Money Laundering Policy (the Policy) was put in place with approval of the Board.

Since then, the Policy has been reviewed and revised with the approval of the Board, in line with the guidelines on KYC & AML issued by regulators.

This policy should be read in conjunction with Suspicious Transaction Detecting and Reporting Policy. Muthoot Housing Finance Company Ltd (MHFCL), which is a registered Housing Finance Company (HFC) with NHB/RBI, provides housing loans, property loans and plot finance to its customers.

MHFCL commits itself to the highest standards of transparency, compliance and fair practices while meeting the business loan needs of Housing in a timely and effective manner. It intends that the HFC's (MHFCL) business, be conducted in accordance with the prevailing statutory and regulatory requirements with due focus on efficiency, customer-orientation and corporate governance principles.

MHFCL shall adopt all the best practices prescribed by NHB/RBI from time to time and shall make appropriate modifications if any necessary to this code to conform to the standards so prescribed. This policy is applicable across all branches / business segments of MHFCL

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, Regulated Entities (HFC) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account- based relationship or otherwise and monitor their transactions. HFC shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s).

In exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act *ibid,* Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India has issued Master Directions which every HFC should follow.

CHAPTER – I: PRELIMINARY

1. Objectives

The basic objectives of the policy are

a. To enable adherence to the "Know Your Customer" (KYC) policies and procedures issued by NHB/RBI

b. To comply with the guidelines issued in Prevention of Money Laundering Act (PMLA), 2002.

2. Applicability

It may be noted that KYC – AML policy as stated in this document shall prevail over anything else contained in any other document / process/circular/letter/instruction in this regard (KYC- AML). This policy shall be applicable to all verticals/products of MHFCL whether existing or rolled out in future.

KYC and AML Policy guidelines are applicable to all the functions of the MHFCL dealing with customers, vendors / service providers and employees. Functions should adhere to the guidelines mentioned in this policy and also incorporate them while designing other internal policies, procedures, products etc.

This policy should be read in conjunction with related internal operational guidelines issued by NHB/RBI from time to time.

3. Definitions:

In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i. "Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

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

iii. "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv. Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

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

b) Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of capital or profits of the partnership.

c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

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

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

v. "Certified Copy" - Obtaining a certified copy by the RE shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.
Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

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

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

vii. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.
Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

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

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

x. "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.

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

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

xiii. "Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

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

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: -
    (i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
    (ii) property or Municipal tax receipt.
    (iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address.
    (iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.
c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.
d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

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

xvi. "Person" has the same meaning assigned in the Act and includes:

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

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

xviii. "Principal Officer" means an officer at the management level nominated by the RE nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

xix. "Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

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

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

xx. A 'Small Account' means a savings account which is opened in terms of subrule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.

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

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

(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. Correspondent Banking: Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable through accounts and foreign exchange services.

iii. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iv. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.

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

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

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

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

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

vi. "Customer identification" means undertaking the process of CDD.

vii. "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

viii. "IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

ix. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

x. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the MHFCL or meeting the officials of MHFCL.

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

xii. Payable-through accounts: The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

xiii. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xiv. "Regulated Entities" (REs) means.

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks

(StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'.

b. All India Financial Institutions (AIFIs)
c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

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

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

a. "Wire transfer" related definitions
b. Batch transfer: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.
c. Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
d. Beneficiary RE: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary RE and makes the funds available to the beneficiary.
e. Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
f. Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
g. Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
h. Financial Institution: In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
i. Intermediary RE: Intermediary RE refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a *serial* or *cover* payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
j. Ordering RE**:** Ordering RE refers to the financial institution, regulated by the RBI, which

initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

k. Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

l. Serial Payment: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).

m. Straight-through Processing: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

n. Unique transaction reference number: Unique transaction reference number refers to a combination of letters, numbers, or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

o. Wire transfer: 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.

(c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II: GENERAL

1. There is a Know Your Customer (KYC) policy duly approved by the Board of Directors of MHFCL..
MHFCL shall ensure that a group-wide policy is implemented for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003).

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

2. The KYC policy includes following four key elements:

(a) Customer Acceptance Policy.
(b) Risk Management.
(c) Customer Identification Procedures (CIP).
(d) Monitoring of Transactions.

3. Money Laundering and Terrorist Financing Risk Assessment by MHFCL:

(a) MHFCL 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, MHFCL shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with MHFCL from time to time.

(b) The risk assessment by MHFCL shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the HFC. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of MHFCL to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

(d) MHFCL 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. MHFCL shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, MHFCL shall monitor the implementation of the controls and enhance them if necessary.

4. Designated Director*:*

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

5. Principal Officer:

MHFCL has designated Head Credit of the Company as 'Principal Officer'. The name of the Principal Officer so designated, his designation, address and contact details including changes from time to time, shall be communicated to the Director, FIU-IND and also to NHB/RBI.

He shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.

6. Compliance of KYC policy

(a) MHFCL to ensure compliance with KYC Policy through:

i. A senior officer in the rank of Head Operations will constitute as 'Senior Management' for the purpose of KYC compliance.

ii. Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / Zonal Office / Circle Office level.

iii. Independent evaluation of the compliance functions of MHFCL policies and procedures, including legal and regulatory requirements be done by Compliance Division, HO.

iv. Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee.

(b) MHFCL shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER – III: CUSTOMER ACCEPTANCE POLICY

1. MHFCL has formulated a robust Customer Acceptance Policy which aims to verify the identity and address of customer by using reliable, independent source documents, data or information. It will however be ensured that Customer Acceptance Policy does not lead to any customer harassment or leads to denial of financial service to general public especially to those who are financially or socially disadvantaged.

2. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, MHFCL shall ensure that:

(a) No account is opened in anonymous or fictitious/benami name.

(b) No account is opened where the MHFCL 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 MHFCL shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

(c) No transaction or account-based relationship is undertaken without following the CDD procedure.

(d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

(e) Additional information, where such information requirement has not been specified in the internal KYC Policy of the MHFCL, is obtained with the explicit consent of the customer.

(f) MHFCL shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account or avail any other product or service from the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of RBI KYC MD

(j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

(k) Where an equivalent e-document is obtained from the customer, MHFCL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

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

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

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

CHAPTER – IV: RISK MANAGEMENT

1. For Risk Management, MHFCL shall have a risk-based approach which includes the following.

(a) Customers shall be categorised as low, medium, and high-risk category, based on the assessment and risk perception of the MHFCL.

(b) Broad principles may be laid down by the MHFCL for risk-categorisation of customers.

(c) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, 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.

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

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

CHAPTER – V: CUSTOMER IDENTIFICATION PROCEDURE (CIP)

1. MHFCL shall undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.

(b) Carrying out any international money transfer operations for a person who is not an account holder of MHFCL.

(c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When MHFCL has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(g) MHFCL shall ensure that introduction is not to be sought while opening accounts.

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

(a) Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by MHFCL to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised, or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the MHFCL.

CHAPTER – VI: CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

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

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

(a) the Aadhaar number were,

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

(ii) he decides to submit his Aadhaar number voluntarily to MHFCL 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.

(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 MHFCL:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a HFC notified under first proviso to sub-section (1) of section 11A of the PML Act, MHFCL 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 MHFCL.

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

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

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline

verification cannot be carried out, MHFCL shall carry out verification through digital KYC as specified under Annex I.

v) KYC Identifier under clause (ac) above, MHFCL shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of HFC, instead of carrying out digital KYC, MHFCL 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, MHFCL 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 MHFCL and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. MHFCL 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 MHFCL and shall be available for supervisory review.

Explanation 1: MHFCL 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: 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.

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

i. There must be a specific consent from the customer for authentication through OTP.

ii. As a risk-mitigating measure for such accounts, MHFCL shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. MHFCL shall have a board approved policy delineating a robust process of due diligence for dealing with

requests for change of mobile number in such accounts.

iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

iv. the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 (sections of RBI KYC MD) or as per Section 18 (sections of RBI KYC MD V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non- face-to-face mode with any other HFC. Further, while uploading KYC information to CKYCR, MHFCL shall clearly indicate that such accounts are opened using OTP based e-KYC and other HFC shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

ix. MHFCL shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

3. MHFCL may undertake live V-CIP, to be carried out by an official of the MHFCL, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following minimum standards:

(a) V-CIP Infrastructure:

i) MHFCL should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of MHFCL and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with MHFCL only and all the data including video recording is transferred to MHFCL exclusively owned / leased server(s) including cloud server, if any, immediately after the V-

CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of MHFCL.

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

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

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

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

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

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

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

(b) V-CIP Procedure

i) MHFCL shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of MHFCL specially trained for this purpose. 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.

ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the MHFCL. However, in case of call drop / disconnection, fresh session shall be initiated.

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

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

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

vi) The authorised official of MHFCL performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) OTP based Aadhaar e-KYC authentication.

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer.

Equivalent e document of OVD including documents issued through digilocker. MHFCL should ensure to redact or blackout the aadhaar number in terms of section 16

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

e) Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, MHFCL shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining theidentification information through CKYCR / Aadhaar authentication /equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, MHFCL shall ensure that no incremental risk is added due to this.

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

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

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

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

xi) Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

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

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by MHFCL.

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. MHFCL shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

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

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

Part II - CDD Measures for Sole Proprietary firms

1. For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.
2. In addition to the above, any two of the following documents or the equivalent e- documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:
   (a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
   (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
   (c) Sales and income tax returns.
   (d) CST/VAT/ GST certificate (provisional/final).
   (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
   (f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
   (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
   (h) Utility bills such as electricity, water, landline telephone bills, etc.
3. In cases where MHFCL are satisfied that it is not possible to furnish two such documents, MHFCL may, at their discretion, accept only one of those documents as proof of business/activity.
4. Provided MHFCL undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Legal Entities

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

(a) Certificate of incorporation
(b) Memorandum and Articles of Association
(c) Permanent Account Number of the company
(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
(e) Documents, as specified in Section 16 (sections of RBI KYC MD), relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company 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.

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

(a) Registration certificate
(b) Partnership deed
(c) Permanent Account Number of the partnership firm
(d) Documents, as specified in Section 16 (sections of RBI KYC MD), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(e) the names of all the partners; and
(f) address of the registered office, and the principal place of its business, if it is different.

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

(a) Registration certificate
(b) Trust deed
(c) Permanent Account Number or Form No.60 of the trust
(d) Documents, as specified in Section 16 (sections of RBI KYC MD), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(e) the names of the beneficiaries, trustees, settlor and authors of the trust
(f) the address of the registered office of the trust; and
(g) list of trustees and documents, as specified in Section 16 (sections of RBI KYC MD), for those discharging the role as trustee and authorised to transact on behalf of the trust.

Part IV - Identification of Beneficial Owner

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

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

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

Part V - On-going Due Diligence

1. MHFCL 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.
2. The extent of monitoring shall be aligned with the risk category of the customer as per Annexure 2

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

   A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

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

4. **Updation / Periodic Updation of KYC**

   MHFCL shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, 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 from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of MHFCL' internal KYC policy duly approved by the Board of Directors of MHFCL or any committee of the Board to which power has been delegated.

   a) Individuals:

   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 MHFCL, customer's mobile number registered with the MHFCL, ATMs, digital channels (such as online banking / internet banking, mobile application of MHFCL), letter, etc.

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

   Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

   Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. MHFCL shall ensure that the mobile number for Aadhaar

authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals:

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

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

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

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

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

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

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

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

a) MHFCL 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; customers shall submit to the MHFCL 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 MHFCL' end.

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

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

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

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

Part VI - Enhanced Due Diligence Procedure

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

a) In case RE has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. MHFCL shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, MHFCL shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) MHFCL shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

1. Accounts of Politically Exposed Persons (PEPs)

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

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

2. Client accounts opened by professional intermediaries:

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

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

CHAPTER – VII: RECORD MANAGEMENT

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

(a) Maintain all necessary records of transactions between MHFCL and the customer, 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, business correspondence 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.

(h) to 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 such customers are not registered, MHFCL shall register the details on the DARPAN Portal. MHFCL shall also maintain such registration records for a period of five years after the business relationship between the customer and the MHFCL has ended or the account has been closed, whichever is later

CHAPTER – VIII: REPORTING REQUIREMENTS TO FINANICAL INTELLIGENCE UNIT – INDIA

1. MHFCL shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

2. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by HFC which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officer of MHFCL will feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

3. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. MHFCL shall not put any restriction on operations in the accounts where an STR has been filed. MHFCL, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done

4. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

CHAPTER – IX: REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES

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

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

The details of the two lists are as under:

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

https://scsanctions.un.org/ohz5jen-al-qaida.html

ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at

https://scsanctions.un.org/3ppp1en-taliban.htm

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

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

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

2. Obligations under Weapons of Mass Destruction (WMD)

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

(a) MHFCL 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 January 30, 2023, by the Ministry of Finance, Government of India (Annex III of the Master Direction).

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

(c) Further, MHFCL 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, MHFCL shall 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. MHFCL shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) MHFCL 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, MHFCL 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 MHFCL from the CNO, MHFCL shall, without delay, take necessary action to comply with the Order.

(i) 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 MHFCL 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.

3. UNSCR 1718 Sanctions List of Designated Individuals and Entities

MHFCL 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 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, MHFCL 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

A new Section 54A has been introduced requiring MHFCL to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

CHAPTER – X: OTHER INSTRUCTIONS

1. Secrecy Obligations and Sharing of Information:

(a) MHFCL shall maintain secrecy regarding the customer information which arises out of the contractual relationship between MHFCL 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, MHFCL 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 banking 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 MHFCL requires disclosure and

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

(e) MHFCL shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

2. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

MHFCL 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.

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

(b) In terms of provision of Rule 9(1A) of the PML Rules, the REs shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(d) MHFCL shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

(e) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Scheduled Commercial Banks (SCBs) are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. SCBs were initially allowed time up-to February 1, 2017, for uploading data

in respect of accounts opened during January 2017.

REs other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

(f) MHFCL shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

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

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, REs shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updation as specified in paragraph 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

Also, whenever MHFCL obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9(1C) of the PML Rules, the RE shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs MHFCL regarding an update in the KYC record of an existing customer, the MHFCL shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by MHFCL.

(i) MHFCL shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(j) For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, MHFCL 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

(v) MHFCL 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.

3. A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by MHFCL.

4. Introduction of New Technologies

MHFCL 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, MHFCL 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.

5. Quoting of PAN

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

6. Hiring of Employees and Employee training

(a) Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.

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

(c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the MHFCL, regulation and related issues shall be ensured.

Annex I – DIGITAL KYC PROCESS

A. MHFCL 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 MHFCL.

B. The access of the Application shall be controlled by MHFCL, 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 MHFCL to its authorized officials.

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

D. MHFCL 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 MHFCL shall put a water- mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by MHFCL) and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the customer.

E. The Application of the MHFCL 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 where possible 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 watermarking 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 officers registered with MHFCL shall not be used for customer signature. MHFCL 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.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of MHFCL, 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 MHFCL 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 MHFCL 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.

Annex II – RISK CATEGORIES

	Low Risk Customer	Medium Risk Customer	High Risk Customer
Definition	(a) Customers like Salaried people– (b) Customer like Self-employed people belonging to lower economic strata of the society whose accounts show small. balances (c) Wherein only customers basic requirements of verifying the identity and location are to be met.	Customers those are less risky in nature as compare to high risk customers – can be categorised as Medium Risk.	Customers that are likely to pose a higher-than-average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.

List of Customers as per Risk category	(a) Salaried employees whose salary structures are well defined, (b) Salaried employees with cash salary structures (c) self-employed People belonging to lower economic strata of the society whose accounts show small balances and low turnover, (d) Government departments & Government owned companies, regulators and statutory bodies, etc. (e) Micro/Small/Medium enterprises filing regular ITR, good banking relationship, existing trade records with any Financial institutions etc.	(a) Client with over investment of Rs. 50 Lakh where identity and sources of wealth are not supported by public documents like income returns, registered conveyance deeds etc. (b) Clients with sudden spurt in volumes or investment without apparent reasons. (c) Clients who trade in derivatives. (d) Customers having speculative income. (e) Person in business/industry or trading activity where scope or history of unlawful trading / business activity dealings is more, etc.	(a) Non-resident customers, (b) Trusts, charities, NGOs and organizations receiving donations, (c) Companies having close family shareholding or beneficial ownership, (d) Firms with 'sleeping partners', (e) Politically exposed persons (PEPs) of foreign origin, (f) Non-face to face customers, and (g) Those with dubious reputation as per public information available, etc.

Annexure III: Indicative list of Suspicious Transaction

A. Illustrative list of suspicious transactions pertaining to housing loans:

1. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
2. Unnecessarily complex client structure.
3. Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.
4. Customer is reluctant to provide information, data, documents;
5. Submission of false documents, data, purpose of loan, details of accounts;
6. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
7. Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
8. Approaches a branch/office of a HFC, which is away from the customer's residential or business address provided in the loan application, when there is HFC branch/office nearer to the given address; Not applicable if the branch in which customer approaches is in the same city or where customer approaches a branch from another city he is acquiring property in such city. i.e. within Geo limits as defined by Company. f. Unable to explain or satisfy the numerous transfers in the statement of account/ multiple accounts;
9. Initial contribution made through unrelated third party accounts without proper justification;
10. 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;
11. Where transactions do not make economic sense;
12. There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
13. Encashment of loan amount by opening a fictitious bank account;
14. 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;
15. Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase and if transaction is found unreasonable as per market practice;
    - Multiple funding of the same property/dwelling unit;
16. Request for payment made in favour of a third party who has no relation to the transaction;
17. 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.
18. 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;
19. Overpayment of instalments with a request to refund the overpaid amount
20. Investment in real estate at a higher/lower price than expected
21. Client incorporated in countries that permit bearer shares.

B. illustrative list of suspicious transactions pertaining to builder/project loans:

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

GROUP-WIDE AML POLICY

In terms of PML Rules, MHFCL, in conjunction with its RBI-regulated group entities, for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003), shall implement a group-wide programme against money laundering and terror financing, including policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management. Such programs shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Under this policy, the MHFCL is authorised by the Board to define and document the Standard Operating Procedure (SOP) that shall cover all such aspects as prescribed by RBI to adhere to the Group-wide AML policy execution.

REVIEW OF THE POLICY

The Policy is subjected to an annual review by the management and modifications, if any warranted, will be taken up for the approval of the Board. If there are any amendments in the regulations, revision in the policy will be staged for Board's approval immediately, after the amendments are notified by the regulator.

*Kindly note sections reference in the policy pertains to latest RBI Circular of KYC Master Direction