



Know Your Customer & Anti-Money Laundering Policy

REVISION/CHANGE HISTORY

Author	Reviewer	Version No.	Effective Date	Change Description
Head - Operations	BOD	1	06.08.2011	Approved w.e.f 6.8.2011
Head - Operations	BOD	1.1	01.10.2013	Reviewed by the Board on 01.10.2013
Head - Operations	BOD	1.2	11.11.2015	Reviewed by the Board on 11.11.2015
Head - Operations	BOD	1.3	25.07.2017	Reviewed by the Board on 25.07.2017
Head - Operations	CEO	1.4	10.05.2018	Reviewed by the Board on 10.05.2018
Head - Operations	CEO	1.5	27.04.2019	Reviewed by the Board on 27.04.2019
Head - Operations	CEO	1.6	11.07.2020	Reviewed by the Board on 11.07.2020
Head - Operations	CEO	1.7	08.02.2021	Reviewed by the Board on 08.02.2021
Head - Operations	CEO	1.8	30.04.2022	Reviewed by the Board on 30.04.2022
Head - Operations	CEO	1.9	28.04.2023	Inserted a new clause 3.14 as UCIC and change in Principal Officer.

Head - Operations	CEO	2	19.6.2023	Amendment in clause 'Equivalent e-document'. New Clauses inserted under i.e., Customer Acceptance Policy. Amendments in customer due diligence requirements and CFT.
Head - Operations	CEO	2.1	2.11.2023	Reviewed the policy in line with the amendment to the Master Direction on KYC dated October 17, 2023
Head - Operations	CEO	2.2	07.11.2024	- Under Video based Customer Identification Process (V-CIP) Removed "MHFCL can only carry out offline verification of Aadhaar for Identification" Replaced with "MHFCL can carry out both Online and Offline Verification of Aadhaar for Identification during the Digital and Physical journey. - Under Video based Customer Identification Process (V-CIP) Additionally Included the clauses as per RBI-KYC Master Direction The authorised official of the 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: - OTP based Aadhaar e-KYC authentication - Offline Verification of Aadhaar for identification - KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer - Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker. - Under Video based Customer Identification Process (V-CIP) Included the PAN Validation through Digilocker - Under Monitoring of transactions included monitoring by Risk Management Committee once in 6 months. - Preservation of Records- Included the timelines of record preservation for Demat accounts.
Head - Operations	CEO	2.3	05.02.2025	Customer Due Diligence (CDD) procedures to be applied at the UCIC level. Thus, if an existing KYC compliant customer opens another account or avail any other product or service with MHFCL, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned. Under CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR), the following para has been added: Also, whenever the 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 MHFCL 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.
				Under CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR), existing sub-points have been replaced with the following:
				(i) There is a change in the information of the customer as existing in the records of CKYCR; or
				(ii) The KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
				(iii) The validity period of downloaded documents has lapsed; or
				(iv) The 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 client.
Head - Operations	CEO	2.4	05.08.2025	Inserted a new Clause on 'Group-Wide Anti-Money Laundering (AML) Policy'.
Head-Operations	CEO	2.5	27.09.2025	Inserted following para under 'Periodic Updation of KYC'- To ensure timely completion of re-KYC requirements, the system is equipped to generate alerts for customers whose re-KYC is due within one year of the prescribed renewal date. Additionally, SMS notifications will be sent to such customers, advising them to complete their KYC renewal in order to avail any new loans or conduct further transactions with the Company.
Head-Operations	CCO	2.6	25.05.2026	Clause 3.24 — Group - Same statutory base, but a new Explanation added clarifying that, for this policy, 'Group' = Muthoot Pappachan Group and includes all entities consolidated in the group's financial statements — specifically RBI-regulated entities MFL, MHFCL and any other regulated entity within the group. Anchors the new Group-Wide AML section. Chapter III — Third-party EMI/Pre-payment/Foreclosure Payments (NEW) - A whole new sub-clause has been inserted covering payments by relatives, family, employers or any third party Chapter VI Part V (B.1) — Change in Address - Significantly tighter: - Self-declaration of new address obtained. - MHFCL may obtain OVD/deemed OVD at its option.

				• “Any change in address shall trigger a full re-KYC process equivalent to onboarding a new customer.”
				Addition of Chapter VI Part V (B.4) — Communication & Intimation Process
				Chapter VI Part V (B.4) — Now embedded in the formal 3-intimation + 3-reminder schedule
				Annex IV — Indicative List of Suspicious Transactions (split) - Renumbered (now Annex IV) and split into two distinct heads: • **A. Suspicious Transactions Pertaining to Housing Loans** (retained list) • **B. Suspicious Transactions Pertaining to Builder / Project Loans** (a separate set of red flags for the developer/project finance side)
				Group-Wide AML Policy section + revised Group definition (3.24) - Substantive linkage: combined with the new Explanation under Clause 3.24, the Group is now explicitly defined as the Muthoot Pappachan Group including MFL, MHFCL and other RBI-regulated entities. The information-sharing obligation between group entities now has a clear definitional anchor.

INDEX

Preface	8
Chapter I: Preliminary	9
1. Objectives.....	9
2. Applicability.....	9
3. Definitions.....	9
3.1 Customer.....	9
3.2 Walk-in Customer	9
3.3 Designated Director	9
3.4 Officially Valid Document (OVD).....	9
3.5 Offline Verification	10
3.6 Acceptance of Aadhaar as an OVD	10
3.7 Person	10
3.8 Transaction.....	10
3.9 Suspicious Transaction.....	10
3.10 KYC Identifier	11
3.11 Certified Copy	11
3.12 Digital KYC	11
3.14 Equivalent e-document.....	11
3.15 UCIC.....	11
3.16 Beneficial Owner (BO)H	11
3.17 Customer Due Diligence (CDD)	11
3.19 On-going Due Diligence	11
3.20 Periodic Updation	11
3.22 Non-Profit Organisation (NPO)	11
3.23 Central KYC Records Registry (CKYCR)	12
3.24 Group	12
3.25 FATCA.....	12
3.26 Common Reporting Standards (CRS)	12
3.27 Wire Transfer Related Definitions	12
Chapter II: General.....	13
1. KYC Policy Framework.....	13
2. Money Laundering and Terrorist Financing Risk Assessment	13
3. Designated Director	13
4. Principal Officer.....	13
5. Compliance of KYC Policy.....	13
Chapter III: Customer Acceptance Policy.....	15

Chapter IV: Risk Management	17
1. Risk-Based Approach.....	17
2. Customers Requiring Enhanced Due Diligence.....	17
3. Risk Categorisation Parameters	17
Chapter V: Customer Identification Procedure (CIP)	18
Chapter VI: Customer Due Diligence (CDD) Procedure	19
Part I – CDD Procedure for Individuals	19
Aadhaar e-KYC Authentication	19
Part II – CDD Measures for Sole Proprietary Firms.....	19
Part III – CDD Measures for Legal Entities	20
A. Company	20
B. Partnership Firm	20
C. Trust	20
D. Unincorporated Association or Body of Individuals	20
E. Juridical Persons (Government Departments, Societies, Universities, Local Bodies).....	20
Part IV – Identification of Beneficial Owner	20
Part V – On-going Due Diligence and Monitoring of Transactions	21
A. On-going Monitoring	21
B. Periodic Updation of KYC	21
B.1 Individual Customers	21
B.2 Legal Entity Customers	22
B.3 Additional Measures.....	22
B.4 Communication and Intimation Process.....	22
B.5 CKYCR-Based KYC Updates.....	22
Part VI – Enhanced Due Diligence Procedure	22
C. Accounts of Politically Exposed Persons (PEPs)	22
E. Usage of Group Entity Customer Data	23
Chapter VII: Record Management	24
Chapter VIII: Reporting Requirements to FIU-IND	26
1. Cash Transaction Report (CTR)	26
2. Suspicious Transaction Reports (STR)	26
3. Non-Profit Organisation Report.....	26
Chapter IX: Combating Financing of Terrorism & International Obligations.....	27
1. UAPA, 1967	27
2. WMD Act, 2005	27
3. UNSCR 1718 Sanctions List	27
Chapter X: Other Instructions	28
1. Confidentiality of Customer Information.....	28

2. CDD Procedure and Sharing KYC Information with CKYCR	28
3. Unique Customer Identification Code (UCIC)	28
4. Introduction of New Technologies.....	28
5. Quoting of PAN	28
6. Sensitizing Customers	28
7. Hiring of Employees and Employee Training	29
8. Technology Requirements	29
Annex I: Digital KYC Process.....	30
Annex II: Risk Categories.....	31
Annex Iii: Indicative List of Suspicious Transactions	33
A. Suspicious Transactions Pertaining to Housing Loans.....	33
B. Suspicious Transactions Pertaining to Builder/Project Loans.....	33
Group-Wide Anti-Money Laundering (AML) Policy	35
Review of the Policy.....	36

PREFACE

The National Housing Bank (NHB) / Reserve Bank of India (RBI) has advised all Housing Finance Companies (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. In terms of the provisions of the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, Regulated Entities (HFCs) are required to follow certain customer identification procedures while undertaking transactions and monitor their transactions. MHFCL, which is a registered Housing Finance Company 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. As a responsible Housing Finance Company, MHFCL considers it as its moral, social and economic responsibility to prevent the misuse of the financial system for laundering proceeds of criminal activities. Our role in curbing this global reality begins with stringent Know Your Customer procedures. This policy lays down the systems and procedures to help control financial frauds, identify money laundering and suspicious transactions, combat financing of terrorism, and ensure careful scrutiny and monitoring of large value and suspicious transactions.

Money Laundering is the process of concealing financial transactions to make illegitimate money appear legitimate. There are three recognised stages of money laundering: (a) Placement – the physical disposal of cash proceeds derived from illegal activity; (b) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions; (c) Integration – the provision of apparent legitimacy to criminally derived wealth.

CHAPTER I: PRELIMINARY

1. Objectives

The basic objectives of this policy are:

- To enable adherence to the Know Your Customer (KYC) policies and procedures issued by NHB/RBI.
- To comply with the guidelines issued under the Prevention of Money Laundering Act (PMLA), 2002 and Rules thereunder.
- To prevent MHFCL from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.
- To put in place a proper control mechanism for detecting and reporting suspicious transactions in accordance with regulatory and statutory provisions.
- To ensure that all the provisions of PMLA 2002, rules and subsequent amendments are complied with.
- To ensure compliance with guidelines and instructions issued by regulators including FIU-IND and RBI.

The Frequently Asked Questions (FAQs) on KYC may be accessed at: <https://rbi.org.in/Scripts/FAQDisplay.aspx?Id=173>

2. Applicability

This KYC-AML-CFT Policy shall prevail over anything else contained in any other document, process, circular, letter or instruction in this regard. This policy shall be applicable to all verticals and products of MHFCL, whether existing or rolled out in future.

KYC and AML Policy guidelines are applicable to all functions of MHFCL dealing with customers and employees. All functions shall adhere to the guidelines mentioned in this policy while drafting their internal policies, procedures, products, etc.

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

3. Definitions

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

3.1 Customer

A 'Customer' is defined as a person who is engaged in a financial transaction or activity with MHFCL and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.2 Walk-in Customer

'Walk-in Customer' means a person who does not have an account-based relationship with MHFCL, but undertakes transactions with MHFCL.

3.3 Designated Director

"Designated Director" means a person designated by MHFCL to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall include: the Managing Director or a whole-time Director, duly authorised by the Board of Directors.

3.4 Officially Valid Document (OVD)

"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:

- where the customer submits proof of possession of Aadhaar number as an OVD, he/she may submit it in such form as are issued by the Unique Identification Authority of India. The customer shall be asked to redact or blackout the Aadhaar number and MHFCL shall ensure the same.

- where the OVD presented by a foreign national does not contain the details of address, 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: A document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

3.5 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.

3.6 Acceptance of Aadhaar as an OVD

. As per the proviso, whoever submits “proof of possession of Aadhaar number” as an OVD, has to do it in such form as are issued by the Authority. Pursuant to the amendment in KYC Master Directions, ‘Proof of possession of Aadhaar number’ has been added to the list of OVD.

The Authority has notified that delivery of Aadhaar number shall mean and include:

- Aadhaar letter: Issued by the Authority carrying name, address, gender, photo and date of birth details.
- Downloaded Aadhaar (e-Aadhaar): Digitally signed by the Authority as per IT Act, 2000.
- Aadhaar Secure QR Code: A quick response code generated by the Authority.
- Aadhaar Paperless Offline e-KYC: An XML document generated by the Authority.

3.7 Person

In terms of PML Act, a ‘person’ includes:

- i) an individual,
- ii) a Hindu undivided family,
- iii) a company,
- iv) a firm,
- v) an association of persons or a body of individuals, whether incorporated or not,
- vi) every artificial juridical person, not falling within any of the above, and
- vii) any agency, office or branch owned or controlled by any of the above.

3.8 Transaction

“Transaction” means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

- i) opening of an account;
- ii) 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;
- iii) the use of a safety deposit box or any other form of safe deposit;
- iv) entering into any fiduciary relationship;
- v) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- vi) establishing or creating a legal person or legal arrangement.

3.9 Suspicious Transaction

“Suspicious transaction” means a “transaction”, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- 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
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to not have economic rationale or bona-fide purpose; or

- 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 organisation or those who finance or are attempting to finance terrorism.

3.10 KYC Identifier

Means the unique number or code assigned to a customer by the Central KYC Records Registry.

3.11 Certified Copy

Obtaining a certified copy 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 MHFCL.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), 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.

3.12 Digital KYC

“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 MHFCL.

3.14 Equivalent e-document

“Equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

3.15 UCIC

Means Unique Customer Identification Code.

3.16 Beneficial Owner (BO)H

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 (more than 10% of shares/capital/profits) or who exercises control through other means. For partnership firms: more than 10% of capital or profits. For unincorporated associations: more than 15% of property/capital/profits. For trusts: author, trustee, beneficiaries with 10% or more interest and any person exercising ultimate effective control.

3.17 Customer Due Diligence (CDD)

Means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

3.19 On-going Due Diligence

Means regular monitoring of transactions in accounts to ensure that those are consistent with MHFCL’s knowledge about the customers, customers’ business and risk profile, the source of funds/wealth.

3.20 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.

3.22 Non-Profit Organisation (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, that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

3.23 Central KYC Records Registry (CKYCR)

Means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

3.24 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.

Explanation: For the purpose of this policy, 'Group' refers to the Muthoot Pappachan Group and includes all entities that are consolidated in the group's financial statements, particularly RBI-regulated entities such as Muthoot FinCorp Limited (MFL), Muthoot Housing Finance Company Limited (MHFCL), and any other regulated entity within the group. This definition is relevant to the Group-Wide AML Policy section where information sharing among group entities is prescribed.

3.25 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.

3.26 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.

3.27 Wire Transfer Related Definitions

All other expressions unless defined herein shall have the same meaning as assigned under the Banking Regulation Act, 1949, the RBI Act, 1935, the PML Act, 2002, the PML Rules, 2005, the Aadhaar Act, 2016 and regulations made thereunder, or as used in commercial parlance.

CHAPTER II: GENERAL

1. KYC Policy Framework

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

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

The KYC policy incorporates the following four key elements:

- i) Customer Acceptance Policy;
- ii) Risk Management;
- iii) Customer Identification Procedures (CIP); and
- iv) Monitoring of Transactions.

2. Money Laundering and Terrorist Financing Risk Assessment

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 customers, countries or geographic areas, products, services, transactions or delivery channels, etc.

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

The risk assessment shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of MHFCL. The periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board, but shall be reviewed at least half yearly.

The outcome shall be put up to the Board or any committee of the Board and shall be available to competent authorities and self-regulating bodies.

MHFCL shall apply a Risk Based Approach (RBA) for mitigation and management of the risks and shall have Board approved policies, controls and procedures in this regard. The Board/ACB shall periodically review ML/TF risk controls and direct enhancements as needed based on monitoring outcomes and NRA updates.

3. Designated Director

MHFCL has appointed the Whole-Time Director of the Company as the Designated Director in terms of the Prevention of Anti-Money Laundering (Amendment) Rule 2013. He/She will be responsible for overall compliance under PMLA and Rules and Regulations made thereunder. The name, designation, address and contact details including changes from time to time, shall be communicated to the Director, FIU-IND and also to RBI. In no case shall the Principal Officer be nominated as the Designated Director.

4. Principal Officer

MHFCL has designated a senior officer at the management level as Principal Officer (PO). The PO is independent and reports directly to the Senior Management. The PO is responsible for ensuring compliance, monitoring transactions, and sharing information as required under the law/regulations. The name, designation, address and contact details shall be communicated to both FIU-IND and RBI.

5. Compliance of KYC Policy

MHFCL shall ensure compliance with KYC Policy through:

- A senior officer in the rank of Head Operations shall constitute as 'Senior Management' for the purpose of KYC compliance.
- Allocation of responsibility through Office Order for effective implementation at HO / Zonal / Circle Office level.
- Independent evaluation of compliance functions by the Compliance Division, HO.
- Concurrent / internal audit system to verify compliance with KYC/AML policies and submit quarterly audit notes to the Audit Committee.
- MHFCL shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
- A certificate from the Statutory Auditors on compliance with KYC/AML/CFT guidelines shall be obtained at the time of preparation of the Annual Report and kept on record.

CHAPTER III: CUSTOMER ACCEPTANCE POLICY

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. MHFCL shall ensure that:

- No account is opened or transaction conducted in anonymous or fictitious/benami name(s).
- Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable categorisation of customers into low, medium and high risk.
- Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and RBI instructions.
- Additional information, where not specified in internal KYC Policy, is obtained with the explicit consent of the customer.
- CDD procedures to be applied at the UCIC level. If an existing KYC compliant customer opens another account or avails any other product or service with MHFCL, there shall be no need for a fresh CDD exercise for identification.
- Not to undertake any transaction where MHFCL is unable to apply appropriate CDD measures i.e. unable to verify identity or obtain required documents. MHFCL may consider closing an existing account under similar circumstances and shall consider filing an STR if necessary.
- MHFCL shall have suitable systems to ensure that the identity of the customer does not match with any person or entity in the sanction lists circulated by the Reserve Bank.
- Where PAN is obtained, it shall be verified from the verification facility of the issuing authority.

Where payments towards EMI, pre-payments, part-payments, foreclosure amounts, or any other dues are received from a person other than the borrower (including relatives, family members, employers, or any third party), the following shall apply:

- i) If the payment is in cash and the single transaction amount exceeds Rs.50,000, PAN or Form 60 of the payer (third party) shall be obtained and verified, in addition to the borrower's PAN already on record.
- ii) If the aggregate cash payments from a single third party exceed Rs.2,00,000 in a financial year (across all accounts/loans), PAN or Form 60 of the payer shall be obtained if not already collected.
- iii) PAN of the third-party payer shall be verified through any of the following:
 - Income Tax Department's PAN Verification portal (<https://www.incometax.gov.in/iec/foportal/>)
 - NSDL PAN verification facility
 - UTIITSL PAN verification facility
- iv) If the payment is by cheque / NEFT / RTGS / UPI from the third party's bank account, the bank account details and PAN of the payer shall be recorded. PAN verification is mandatory if the single transaction exceeds Rs.50,000.
- v) A declaration shall be obtained from the third-party payer stating the relationship with the borrower and the purpose of payment.
- vi) Where third-party payments are frequent, unusually large, or from parties with no apparent connection to the borrower, the transaction shall be flagged for enhanced scrutiny and may be reported as a Suspicious Transaction if warranted.

- Where an equivalent e-document is obtained, MHFCL shall verify the digital signature as per the provisions of the IT Act, 2000.
- Where GST details are available, the GST number shall be verified from the issuing authority.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.

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. Risk-Based Approach

MHFCL shall adopt a risk-based approach which includes the following:

- Customers shall be categorised as low, medium, and high-risk, based on the assessment and risk perception of MHFCL.
- Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, information about the customer's business and their location, geographical risk, type of products/services, delivery channel, types of transactions (cash, cheque, wire transfers, etc.).
- The risk categorisation and specific reasons shall be kept confidential and shall not be revealed to the customer to avoid tipping off.
- MHFCL's internal audit and compliance functions shall independently evaluate adherence to KYC policies and procedures.
- The internal auditors shall check transactions for compliance with anti-money laundering guidelines and report to the Audit Committee on a quarterly basis.

2. Customers Requiring Enhanced Due Diligence

Customers that are likely to pose a higher-than-average risk shall be categorised as medium or high risk. Examples include:

- Non-resident customers;
- Customers from countries that do not or insufficiently apply FATF standards;
- High net worth individuals;
- Trusts, charities, NGOs and organisations receiving donations;
- Companies having close family shareholding or beneficial ownership;
- Firms with 'sleeping partners';
- Politically exposed persons (PEPs);
- Non-face to face customers; and
- Those with dubious reputation as per public information available.

Only NPOs/NGOs promoted by United Nations or its agencies shall be classified as low risk customers.

3. Risk Categorisation Parameters

Detailed risk categories are provided in [Annex II](#) of this policy.

CHAPTER V: CUSTOMER IDENTIFICATION PROCEDURE (CIP)

MHFCL shall undertake identification of customers in the following cases:

- Commencement of an account-based relationship with the customer.
- When there is a doubt about the authenticity or adequacy of the customer identification data.
- Selling third party products as agents, selling 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.
- Carrying out transactions for a walk-in customer where the amount equals or exceeds rupees fifty thousand, whether single or connected transactions.
- When MHFCL has reason to believe that a customer is intentionally structuring transactions below the threshold of rupees fifty thousand.

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

CHAPTER VI: CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

Part I – CDD Procedure for Individuals

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, authorised signatory or the power of attorney holder related to any legal entity:

- The Aadhaar number (where applicable under Aadhaar Act, 2016 or voluntarily submitted);
- The proof of possession of Aadhaar number where offline verification can be carried out; or
- 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 identity and address;
- The KYC Identifier with explicit consent to download records from CKYCR; and
- The Permanent Account Number or the equivalent e-document thereof or Form No. 60; and
- Such other documents including in respect of the nature of business and financial status.

Where the customer has submitted proof of possession of Aadhaar where offline verification can be carried out, MHFCL shall carry out offline verification. Where an equivalent e-document of any OVD is submitted, MHFCL shall verify the digital signature and take a live photo as specified under [Annex I](#) (Digital KYC).

Where any OVD or proof of possession of Aadhaar where offline verification cannot be carried out is submitted, MHFCL shall carry out verification through Digital KYC as specified under [Annex I](#).

Aadhaar e-KYC Authentication

MHFCL shall, at the time of receipt of the Aadhaar number, carry out with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.

Provided that:

- Yes/No authentication shall not be carried out while establishing an account-based relationship.
- For existing accounts with Yes/No authentication, biometric or OTP based e-KYC authentication shall be carried out within six months.
- Yes/No authentication for beneficial owners of a legal entity shall suffice for existing accounts or while establishing a new relationship.
- Where OTP based authentication is performed in non-face to face mode for new accounts, MHFCL shall ensure the mobile number for Aadhaar authentication matches the one in the customer's profile.
- Biometric based e-KYC authentication including Aadhaar Face Authentication can be done by officials or business correspondents.

Failing which, the account shall cease to be operational. In case of loan accounts, only credits shall be allowed.

KYC verification once done by one branch of MHFCL shall be valid for transfer to any other branch, provided full KYC has been done and is not due for periodic updation.

Part II – CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out. In addition, any two of the following documents as proof of business/activity shall also be obtained:

- Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
- Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
- Sales and income tax returns.

- GST certificate.
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
- IEC issued to the proprietary concern by DGFT or licence/certificate of practice issued by any professional body incorporated under a statute.
- Complete Income Tax Return in the name of the sole proprietor where the firm's income is reflected.
- Utility bills such as electricity, water, landline telephone bills.

In cases where it is not possible to furnish two documents, MHFCL may at its discretion accept only one, provided it undertakes contact point verification and satisfies itself of the business activity.

Part III – CDD Measures for Legal Entities

A. Company

Certified copies of: Certificate of incorporation; Memorandum and Articles of Association; PAN of the company; Board resolution and power of attorney; Documents relating to beneficial owner, managers, officers holding authority to transact; names of persons holding senior management position; registered office and principal place of business.

B. Partnership Firm

Certified copies of: Registration certificate; Partnership deed; PAN of the partnership firm; Documents relating to beneficial owner and persons holding authority; names of all partners; registered office and principal place of business.

C. Trust

Certified copies of: Registration certificate; Trust deed; PAN or Form No. 60 of the trust; Documents relating to beneficial owner and persons holding authority; names of beneficiaries, trustees, settlor and authors; registered office; list of trustees and their documents.

D. Unincorporated Association or Body of Individuals

Resolution of the managing body; Power of attorney; Documents relating to beneficial owner and attorney holders; information to establish legal existence; names of all partners; registered office and principal place of business.

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

E. Juridical Persons (Government Departments, Societies, Universities, Local Bodies)

Document showing name of authorised person; Aadhaar/PAN/OVD for the authorised person; documents to establish legal existence.

Part IV – Identification of Beneficial Owner

When MHFCL identifies a customer for opening a business relationship, it shall identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules & Section 89 & 90 of Companies Act 2013 to verify his identity:

- Company: Natural person(s) with controlling ownership interest (>10% of shares/capital/profits) or control.
- Partnership firm: Natural person(s) with >10% of capital or profits.
- Unincorporated association/body: Natural person(s) with >15% of property/capital/profits.
- Where no natural person identified, the relevant person holding the position of senior managing official.
- Trust: Author, trustee, beneficiaries with 10%+ interest, and any person exercising ultimate effective control.
- Listed companies and their subsidiaries: Not necessary to identify shareholders/beneficial owners.

In cases of trust/nominee or fiduciary accounts, MHFCL shall determine whether the customer is acting on behalf of another person and obtain satisfactory evidence of identity of intermediaries and persons on whose behalf they are acting.

Part V – On-going Due Diligence and Monitoring of Transactions

A. On-going Monitoring

MHFCL shall undertake on-going due diligence to ensure transactions are consistent with knowledge about the customers. The following types of transactions shall be closely monitored:

- Large and complex transactions including RTGS transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
- Transactions which exceed the thresholds prescribed for specific categories of accounts.
- Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
- High account turnover inconsistent with the size of the balance maintained.
- Deposit of third-party cheques, drafts, etc. in existing and newly opened accounts followed by cash withdrawals.
- Large number of transactions inconsistent with the profile of the customer.
- Transactions in accounts of marketing firms, especially Multi-level Marketing (MLM) companies, shall be closely monitored.

For ongoing due diligence, MHFCL may consider adopting appropriate innovations including Artificial Intelligence and Machine Learning (AI & ML) technologies to support effective monitoring.

The extent of monitoring shall be aligned with the risk category. A system of periodic review of risk categorisation, at least once in six months, shall be put in place. The Board/ACB shall periodically review ML/TF risk controls and direct enhancements as needed.

B. Periodic Updation of KYC

MHFCL shall adopt a risk-based approach for periodic KYC updation:

- High-risk customers: Every 2 years.
- Medium-risk customers: Every 8 years.
- Low-risk customers: Every 10 years.

Timeline shall be calculated from the date of account opening or last KYC updation, whichever is later.

For low-risk individual customers, KYC may be updated within one year of falling due or up to 30 June 2026, whichever is later, with self-declaration/positive confirmation options.

B.1 Individual Customers

No Change in KYC Information: Customer shall submit self-declaration via registered email, registered mobile, mobile application, or physical letter.

Change in Address: Self-declaration of new address shall be obtained. MHFCL may at its option obtain OVD/deemed OVD for address verification. In accordance with MHFCL's internal policy, any change in address shall trigger a full re-KYC process equivalent to onboarding a new customer.

Aadhaar OTP-based e-KYC: May be used for periodic updation in non-face-to-face mode. Declaration of current address, if different from Aadhaar address, shall not require positive confirmation. Mobile number for authentication must match the one in customer's profile.

Business Correspondents (BCs): MHFCL may utilise authorised BCs to facilitate KYC updation. BCs may collect self-declarations and supporting documents. After biometric-based e-KYC authentication, BCs shall forward documents to the concerned branch and provide acknowledgment to the customer. The ultimate responsibility remains with MHFCL.

Minor to Major Transition: Fresh photographs and updated CDD documents shall be obtained upon customer attaining majority.

B.2 Legal Entity Customers

No Change: Self-declaration from authorised official or board resolution via registered email, mobile application, or physical letter. MHFCL shall verify and update Beneficial Ownership information.

Change in KYC Information: Full KYC process equivalent to onboarding a new LE customer shall be undertaken.

B.3 Additional Measures

- CDD documents must comply with current standards even if no change in customer information.
- If validity of existing CDD documents has expired, a full KYC process shall be undertaken.
- PAN details shall be verified against the issuing authority's database.
- Acknowledgment shall be provided to the customer indicating the date of updation.
- All updated information shall be promptly recorded and customer informed of the date of KYC updation.
- MHFCL may offer KYC updation services at any branch.

B.4 Communication and Intimation Process

MHFCL shall issue:

- At least three advance intimations prior to the due date, including at least one by letter:
 - First intimation: 60 days prior to due date via SMS, email, or app notification.
 - Second intimation: 30 days prior to due date through a physical letter.
 - Third intimation: 7 days before due date via SMS, email, or app notification.
- If the customer fails to comply after the due date, at least three reminders including one by letter:
 - First reminder: 7 days after due date via SMS or email.
 - Second reminder: 15 days after due date through a physical letter.
 - Third reminder: 30 days after due date via SMS, email, or app notification.

Each communication shall include clear instructions for updating KYC, escalation mechanism for assistance, and consequences of non-compliance. All communications shall be recorded for audit trail. To be implemented no later than January 1, 2026.

B.5 CKYCR-Based KYC Updates

MHFCL shall update customers' KYC records based on update notifications received from the Central KYC Records Registry (CKYCR). Whenever MHFCL obtains additional or updated information, it shall within seven days furnish the updated information to CKYCR.

Part VI – Enhanced Due Diligence Procedure

C. Accounts of Politically Exposed Persons (PEPs)

MHFCL shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from normal CDD:

- Appropriate risk management systems to determine whether the customer or beneficial owner is a PEP.
- Reasonable measures for establishing source of funds/wealth.
- Approval to open account shall be obtained from senior management.
- All such accounts subjected to enhanced monitoring on an ongoing basis.
- If an existing customer or beneficial owner subsequently becomes a PEP, senior management's approval shall be obtained to continue the relationship.

These instructions shall also apply to family members or close associates of PEPs.

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

E. Usage of Group Entity Customer Data

MHFCL may make use of the customer data of the group entities for cross selling and/or for any other purpose provided that each of the group entities had previously taken express approval from their customers in this regard.

CHAPTER VII: RECORD MANAGEMENT

MHFCL shall take the following steps regarding maintenance, preservation and reporting of customer information:

- Maintain all necessary records of transactions between MHFCL and the customer, both domestic and international, for at least five years from the date of transaction.
- Preserve the records pertaining to the identification of 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.
- Make available swiftly the identification records, business correspondence and transaction data to the competent authorities upon request.
- Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules, 2005, including:
 - All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
 - Series of all cash transactions individually valued below Rupees Ten Lakh within a month where monthly aggregate exceeds Rupees Ten Lakh;
 - All transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh;
 - All cash transactions where forged or counterfeit currency notes have been used as genuine;
 - All suspicious transactions, whether or not in cash.
- Maintain all necessary information to permit reconstruction of individual transactions (nature, amount, currency, date, parties).
- Evolve a system for proper maintenance and preservation in a manner that allows data to be retrieved easily and quickly.
- Maintain records in hard or soft format.
- Pay special attention to all complex, unusual large transactions and unusual patterns with no apparent economic or visible lawful purpose. Background including all documents/records shall be examined and findings properly recorded.
- In case of customers who are NPOs, ensure details are registered on the DARPAN Portal of NITI Aayog and maintain such records for five years after the business relationship has ended or account has been closed, whichever is later.

Clarification on Cash Transaction Threshold and Reporting

- i) The Rs.10 Lakh threshold for recording cash transactions applies both to single transactions and to a series of integrally connected transactions.
- ii) 'Integrally connected transactions' means all cash transactions across ALL accounts and loans of the same customer, identified by UCIC, aggregated within a calendar month.
- iii) Where a single customer (individual, HUF, company, partnership, or any other person) makes multiple cash payments across different loan accounts, all such payments shall be aggregated under the customer's UCIC for the purpose of determining whether the Rs.10 Lakh threshold is breached.
- iv) The aggregation shall include cash receipts towards EMI payments, pre-payments, part-payments, foreclosure amounts, margin money deposits, processing fee payments, and any other cash receipts from the customer.
- v) The Cash Transaction Report (CTR) shall be filed monthly to FIU-IND by the 15th of the succeeding month.

- vi) The Counterfeit Currency Report (CCR) shall also be filed by the 15th of the succeeding month where forged or counterfeit currency notes have been detected.
- vii) The Principal Officer shall sign the monthly summary and ensure timely filing. A copy of the CTR shall be retained at the concerned branch for production to auditors and inspectors.

This Chapter should be read in conjunction with the Board approved Policy on Preservation of Documents, Customer Documents Retention and Destruction of Records.

CHAPTER VIII: REPORTING REQUIREMENTS TO FIU-IND

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

1. Cash Transaction Report (CTR)

- The CTR for each month shall be submitted to FIU-IND by 15th of the succeeding month.
- All cash transactions where forged or counterfeit Indian currency notes have been used shall be reported in CCR format by 15th of the next month.
- Details of individual transactions below Rupees Fifty Thousand need not be furnished.
- CTR shall contain only transactions carried out by MHFCL on behalf of its customers.
- A summary signed by the Principal Officer shall be submitted to FIU-IND.
- A copy of monthly CTR shall be available at branches for production to auditors/inspectors.

2. Suspicious Transaction Reports (STR)

- MHFCL shall be guided by the definition of suspicious transaction as contained in PMLA Rules.
- The fact of furnishing STR shall be kept strictly confidential.
- Attempted transactions shall also be reported in STRs, irrespective of amount.
- STRs shall be filed if there is reasonable ground to believe the transaction involves proceeds of crime, irrespective of the amount.
- STR shall be furnished within seven days of arriving at a conclusion that any transaction is suspicious.
- MHFCL shall not put any restrictions on operations in accounts where an STR has been filed.

Delay of each day in not reporting or rectifying shall constitute a separate violation.

Robust software throwing alerts when transactions are inconsistent with risk categorisation and updated customer profile shall be deployed.

3. Non-Profit Organisation Report

All transactions involving receipts by NPOs of value more than Rupees Ten Lakh shall be submitted monthly to FIU-IND by 15th of the succeeding month in prescribed format.

CHAPTER IX: COMBATING FINANCING OF TERRORISM & INTERNATIONAL OBLIGATIONS

1. UAPA, 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 UNSC sanctions lists:

- The “ISIL (Da’esh) & Al-Qaida Sanctions List” (resolutions 1267/1989/2253).
- The “Taliban Sanctions List” (resolution 1988 (2011)).

MHFCL shall also refer to lists in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007. These lists shall be verified on a daily basis and any modifications shall be taken into account for meticulous compliance.

Details of accounts resembling any individuals/entities shall be reported to FIU-IND and MHA. The procedure for freezing of assets under Section 51A shall be strictly followed.

2. WMD Act, 2005

MHFCL shall ensure meticulous compliance with Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005:

- Shall not carry out transactions where particulars match the designated list.
- Shall run checks at the time of establishing a relationship and periodically.
- In case of match, immediately inform the Central Nodal Officer (CNO), State Nodal Officer, and RBI. File STR with FIU-IND.
- Shall prevent matched individuals/entities from conducting financial transactions under intimation to the CNO without delay.
- Shall comply with any freeze order received from CNO without delay.
- Unfreezing shall be observed as per paragraph 7 of the Order.

3. UNSCR 1718 Sanctions List

MHFCL shall verify every day the ‘UNSCR 1718 Sanctions List of Designated Individuals and Entities’ available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm> and ensure compliance with the Implementation of Security Council Resolution on Democratic People’s Republic of Korea Order, 2017.

In addition, MHFCL shall take into account other UNSCRs and lists in the first and fourth schedules of UAPA, 1967.

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

CHAPTER X: OTHER INSTRUCTIONS

1. Confidentiality of Customer Information

MHFCL shall maintain secrecy regarding customer information arising from the contractual relationship. Information collected for opening of account shall be treated as confidential and not divulged for cross selling or any other purpose without express permission.

Exceptions to the secrecy rule:

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

2. CDD Procedure and Sharing KYC Information with CKYCR

MHFCL shall capture the KYC information for sharing with CKYCR as per KYC templates for 'Individuals' and 'Legal Entities'.

- Upload customer's KYC records within 10 days of commencement of an account-based relationship.
- Upload KYC records pertaining to LEs opened on or after April 1, 2021.
- Communicate KYC Identifier to the individual/LE once generated.
- Upload/update KYC data pertaining to older accounts at the time of periodic updation.
- Whenever additional or updated information is obtained, furnish to CKYCR within seven days.
- Ensure during periodic updation that customers are migrated to the current CDD standard.

Where a customer submits a KYC Identifier with consent to download from CKYCR, MHFCL shall retrieve records online and the customer shall not be required to submit the same again unless: there is a change in information; the record is incomplete or not current; validity has lapsed; or MHFCL considers it necessary for verification or enhanced due diligence.

Explanation: The RE that has last uploaded or updated the customer's KYC records in CKYCR shall be responsible for verifying identity and/or address. Any NBFC downloading and relying on such records shall not be required to re-verify, provided the records are current and compliant.

3. Unique Customer Identification Code (UCIC)

A UCIC shall be allotted while entering into new relationships with individual customers as also the existing customers. MHFCL may at its option not issue UCIC to all walk-in/occasional customers, provided adequate mechanisms exist to identify frequent walk-in customers and allot UCIC to them.

4. Introduction of New Technologies

MHFCL shall identify and assess the ML/TF risks that may arise in relation to new products, new business practices, new delivery mechanisms, and use of new or developing technologies. MHFCL shall ensure:

- ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies.
- Adoption of a risk-based approach to manage and mitigate risks through appropriate EDD measures and transaction monitoring.

5. Quoting of PAN

PAN or equivalent e-document thereof shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN.

6. Sensitizing Customers

MHFCL shall prepare specific literature/pamphlets to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited. The front desk staff shall be specially trained to handle such situations.

7. Hiring of Employees and Employee Training

- Adequate screening mechanism, including Know Your Employee/Staff policy, as an integral part of personnel recruitment/hiring process shall be put in place.
- Screening of existing employees at regular intervals (bi-annually) shall be done by the HR department and results shared with the compliance department.
- MHFCL shall ensure staff dealing with KYC/AML/CFT have high integrity, ethical standards, good understanding of KYC/AML/CFT, effective communication skills, and ability to keep up with the changing landscape.
- On-going employee training programme shall be put in place. Focus shall be different for frontline staff, compliance staff and staff dealing with new customers.
- Regular communication through email and portal shall be made available for effective compliance guidance.

8. Technology Requirements

The AML software deployed by MHFCL shall be comprehensive and robust enough to capture all cash and relevant transactions. Robust software throwing alerts when transactions are inconsistent with risk categorisation shall be deployed as part of effective identification and reporting.

ANNEX I: DIGITAL KYC PROCESS

MHFCL shall develop an application for digital KYC process which shall be made available at customer touch points. The KYC process shall be undertaken only through this authenticated application.

- i) The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given to authorised officials.
- ii) The customer, for the purpose of KYC, shall visit the location of the authorised official or vice-versa. The original OVD shall be in possession of the customer.
- iii) MHFCL shall ensure that the live photograph of the customer is taken by the authorised officer and embedded in the Customer Application Form (CAF). The system shall put a watermark in readable form having CAF number, GPS coordinates, authorised official's name, unique employee Code, Date (DD:MM:YYYY) and time stamp (HH:MM:SS).
- iv) The Application shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph is accepted. The background shall be of white colour and no other person shall come into the frame.
- v) The live photograph of the original OVD or proof of possession of Aadhaar (placed horizontally) shall be captured vertically from above with watermarking. No skew or tilt in the mobile device shall be there.
- vi) The live photographs shall be captured in proper light so that they are clearly readable and identifiable.
- vii) All entries in the CAF shall be filled as per documents and information furnished. Where QR code is available, details can be auto-populated by scanning.
- viii) Upon completion, an OTP shall be sent to the customer's own mobile number. Upon successful validation, it will be treated as customer signature on CAF. The mobile number of the authorised officer shall not be used for customer signature.
- ix) The authorised officer shall provide a declaration verified with OTP sent to his registered mobile number. The live photograph of the authorised official shall also be captured.
- x) The Application shall generate a transaction-id/reference-id number. The authorised officer shall intimate the details to the customer for future reference.
- xi) The authorised officer shall verify that: (i) information in the document matches the CAF; (ii) live photograph matches the photo in the document; and (iii) all necessary details including mandatory fields are filled properly.
- xii) On successful verification, the CAF shall be digitally signed by the authorised officer who will take a print, get signatures/thumb-impression of customer, then scan and upload the same. 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. (a) Salaried employees whose salary structures are well defined,	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	(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.
--	---	--	---

ANNEX III: INDICATIVE LIST OF SUSPICIOUS TRANSACTIONS

A. Suspicious Transactions Pertaining to Housing Loans

- Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- Unnecessarily complex client structure.
- Individual or classes of transactions that take place outside the established business profile.
- Customer is reluctant to provide information, data, documents.
- Submission of false documents, data, purpose of loan, details of accounts.
- Refuses to furnish details of source of funds by which initial contribution is made; sources of funds are doubtful.
- Reluctant to meet in person; represents through a third party/Power of Attorney holder without sufficient reasons.
- Approaches a branch/office away from the customer's residential or business address without valid reason (not applicable if branch is in the same city or where customer is acquiring property in such city, i.e. within geo-limits as defined by MHFCL).
- Unable to explain numerous transfers in the statement of account or multiple accounts.
- Initial contribution made through unrelated third party accounts without proper justification.
- Availing top-up loan and/or equity loan without proper justification of end use.
- Suggesting dubious means for sanction of loan.
- Transactions that do not make economic sense.
- Reasonable doubts over the real beneficiary of the loan and the property to be purchased.
- Encashment of loan amount by opening a fictitious bank account.
- Applying for a loan knowing the property has been funded earlier and is outstanding.
- Sale consideration stated in the agreement is abnormally higher/lower than prevailing in the area.
- Multiple funding of the same property/dwelling unit.
- Request for payment made in favour of a third party who has no relation to the transaction.
- Usage of loan amount in connivance with vendor/builder/developer/broker for purposes other than stipulated.
- Multiple funding/financing involving NGO/Charitable Organisation/SMEs/SHGs/MFGs.
- Frequent requests for change of address.
- Overpayment of instalments with a request to refund the overpaid amount.
- Investment in real estate at a higher/lower price than expected.
- Client incorporated in countries that permit bearer shares.

B. Suspicious Transactions Pertaining to Builder/Project Loans

- Builder approaching for a small loan compared to the total cost of the project.
- Builder unable to explain the sources of funding for the project.
- Approvals/sanctions from various authorities are proved to be fake.
- Management appears to be acting according to instructions of unknown or inappropriate person(s).
- Employee numbers or structure inconsistent with size or nature of the business.
- Clients with multi-jurisdictional operations without adequate centralised corporate oversight.
- Advice on setting up legal arrangements to obscure ownership or real economic purpose.

- Entities with a high level of transactions in cash or readily transferable assets.

GROUP-WIDE ANTI-MONEY LAUNDERING (AML) POLICY

In accordance with the Prevention of Money Laundering (PML) Act, 2002 and in alignment with the regulations set forth by the Reserve Bank of India (RBI), MHFCL, along with its RBI-regulated group entities, shall implement a comprehensive group-wide programme aimed at combating money laundering and terrorist financing. This programme will include policies for the sharing of information necessary for client due diligence, as well as for managing money laundering and terrorist financing risks.

The programme will establish strict protocols to ensure the confidentiality and appropriate use of exchanged information, with specific safeguards to prevent unauthorised disclosure or tipping-off.

Under this policy, the Board has authorised the AML Committee to define and document the Standard Operating Procedures (SOP) that will guide the execution of the group-wide AML programme.

The following broad guidelines shall be followed for information sharing among the RBI-regulated group entities:

- i) All REs of the Muthoot Pappachan Group shall share information among each other relating to transactions, accounts, customer details that are deemed suspicious or barred from ML or TF perspective, in such manner and with such safeguards as may be decided by the respective AML Committee.
- ii) On receipt of such information, every RE shall ensure that the information is treated in strict confidence and used only for the purpose of detection of transactions relating to ML and/or TF.

How to share information:

When the AML Committee decides to report any case under CTR/STR, the following information shall be shared with all REs in the Group:

- The nature of the transaction.
- The reasons that led to the decision to report under CTR/STR.
- Minimal Personally Identifiable Information (PII) data required by the group entity to trace if it has any exposure on the same customer.

The Principal Officer shall communicate the information to POs of all REs in the Group in strict confidence.

REVIEW OF THE POLICY

This policy shall be reviewed at least once in a financial year 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.

Note: Paragraph references in this policy pertain to the latest RBI Master Direction – Know Your Customer (KYC) Direction, 2016 (Updated as on June 12, 2025), updated from time to time.

