HINDUJA LEYLAND FINANCE

KYC & AML Policy

HINDUJA LEYLAND FINANCE

Contents

HINDUJA LEYLAND FINANCE

KYC & AML POLICY

Introduction:

KYC (Know Your Customer) is the platform on which the company operates to avoid shortcomings in operational, legal and reputation risks to the institution and the consequential losses by scrupulously following various procedures laid down for opening and conduct of accounts. Money laundering is involvement in any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities including drug trafficking, armed robbery, tax evasion, smuggling, etc. KYC guidelines are accepted internationally as an important anti-money laundering measure.

In compliance with the guidelines issued by RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025) from time to time, the following AML & KYC Policy of the Company is approved by the Board of Directors of the Company.

Where applicable laws and regulations prohibit implementation of these RBI guidelines, HLF shall bring it to the notice of the Reserve Bank of India for further necessary action by HLF including application of additional measures to be taken by the HLF to manage the ML/TF risks.

Objectives:

The policy framework of the Company shall seek 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, it shall also be considered to adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better."

Implementation of Group-wide Policy:

In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003). Accordingly, HLF shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Explanation -

"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).

AML Policy:

The primary objective of the policy is to prevent the company from being used intentionally/ unintentionally by criminal elements for money laundering or terrorist financing activities. The policy seeks:

i) To prevent the criminals from using the company for money laundering activities
ii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with the applicable laws and laid down procedures
iii) To promote compliance with laws pertaining to financial sector
iv) To eliminate the risk that the company will be used for illicit or illegal activities
v) To prevent placement/ layering/ integration of proceeds of crime into the company's finances
vi) To reduce the risk of government seizure and forfeiture of a client's loan collateral when the customer is involved in criminal activity
vii) To protect the company's reputation
viii) To check misappropriations
ix) To weed out undesirable customer
x) To avoid opening of accounts with fictitious names and addresses
xi) To monitor transactions of suspicious nature
xii) To ensure that employees of the company are adequately trained in KYC/ AML/ CFT procedures.

Definition of Money Laundering:

Rule 3 of Prevention of Money Laundering Act (PMLA) defines "the offence of money laundering" as follows:

"Whomsoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering". The process involves creating a web of financial transactions so as to hide the true nature and origin of funds. For the purpose of this policy, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

Obligations under PMLA:

Section 12 of PMLA requires every financial intermediary maintain a record of prescribed transactions

To furnish information of prescribed transactions to the specified authority

To verify and maintain records of the identity of its clients

To preserve records in respect of the above for a period of ten years from the date of cessation of the transactions with the clients.

"Suspicious transaction" means a transaction 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 have no economic rationale or bonafide purpose; or

(d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Key Elements of the KYC Policy

KYC Policy includes the following nine key elements:

1. Customer Acceptance Policy (CAP)
2. Customer Identification Procedures (CIP)
3. Monitoring of Transactions
4. Risk management
5. Training Program
6. Internal Control Systems
7. Record Keeping
8. Assessment and Review
9. Introduction of new technologies
10. Duties / Responsibilities and Accountability – Principal Nodal Officer

1. Customer Acceptance Policy:

It lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship are as follows:

i) No account/ contracts are to be opened/ entered in anonymous or fictitious/benami name(s)/entity (ies)

ii) No account/ contracts are opened/ entered where the company is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. HLF may consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

iii) Accept customers only after verifying their identity, as laid down in Customer identification Procedures.

iv) Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization.

v) Documentation requirements and other information to be collected, as per PMLA and RBI guidelines/instructions, to be complied with

vi) Not to open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed due to non-cooperation of the customer

vii) Identity of a new customer to be checked so as to ensure that it does not match with any person/entity with known criminal background or banned entities such as individual terrorists or terrorist organizations available in the sanctions lists.

viii) The decision to open an account for Politically Exposed Person (PEP) should be taken at a senior management level. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer/ the company. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

Explanation: For the purpose of this paragraph, '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.

ix) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be strictly followed.

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

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

xii) Where a GST is obtained from customer, the company may verify the Goods and Services Tax (GST) number from the search / verification facility of the issuing authority, where the GST details are available.

xiii) Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.

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

xv) apply the CDD procedure at the Unique Customer Identification Customer (UCIC) level. Thus, if an existing KYC-compliant customer of an NBFC desires to open another account or avail of any

other product or service from the same NBFC, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

Customer Acceptance Policy requirements for various categories of customers:

A) Trust/Nominee or Fiduciary Accounts:

Branch/offices should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branch/offices may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

While opening an account for a trust, branches/offices should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined.

In the case of a "Foundation', branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

B) Accounts of Companies and Firms

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with the company. Branch/ office may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g., in the case of a public company it will not be necessary to identify all the shareholders.

C) Client Accounts Opened by Professional Intermediaries:

When the Branch/office has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

Branch/office also maintains 'pooled' accounts managed by lawyers/ chartered accountants for funds held on deposit' for a range of clients.

Where funds held by the intermediaries are not co-mingled at the Branch/office and there are 'sub-accounts', each of them attributable to beneficial owner, all the beneficial owners must be identified.

Where such funds are co-mingled at the Branch/office, the company should still look through to the beneficial owners. Where the Branch/ office rely on the 'customer due diligence' (CDD) means identifying and verifying the customer and the beneficial owner done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

It should be understood that the ultimate responsibility for knowing the customer lies with the Branch/office.

D) Adherence To Foreign Contribution Regulation Act (FCRA), 2010

Branches/Offices should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 2010 cautioning them to open accounts or collect cheques only in favour of association, which are registered under the Act abide by Government of India. A certificate to the effect that the association is registered with the Government of India should be obtained from the concerned associations at the time of opening of the account or collection of cheques. Branches/offices are advised to exercise due care to ensure compliance and desist from opening accounts in the name of banned organizations and those without requisite registration.

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

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, HLF 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. HLF 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.

d) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. HLF shall be 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. HLF 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.

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

f) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, HLF 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 the HLF obtains additional or updated information from any customer as per clause in paragraph 58 of KYC Master Direction or Rule 9 (1C) of the PML Rules, HLF 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 HLF regarding an update in the KYC record of an existing customer, the HLF shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the HLF.

g) HLF shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

h) For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, HLF shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

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

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

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

   (iv) HLF 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.

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

F. Accounts of Politically Exposed Persons (PEPs) Resident Outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branch/office should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

Branch/office should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior management level and should be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

HLF have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP:

1. Reasonable measures shall be taken by HLF for establishing the source of funds / wealth;
2. All such accounts are subjected to enhanced monitoring on an on- going basis;
3. In the event of an existing customer or the beneficial owner of an existing account subsequently

becoming a PEP, senior management's approval is obtained to continue the business relationship;

Unique Customer Identification Code (UCIC):

a) A UCIC shall be allotted while entering into new relationships with individual customers as also the existing individual customers by HLF.
b) The HLF shall, at their option, not issue UCIC to all walk-in / occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

Risk categorization of Customer Profile:

For risk management, the NBFC shall have a risk-based approach which includes the following.

The company shall categorise customers into low, medium, and high-risk categories, based on its assessment and risk perception

Branches/offices should prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients, business and their location etc.

Low Risk:

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk.

Few examples of low-risk customers are:

a) Salaried employees whose salary structure is well-defined
b) People belonging to lower economic strata of the society whose accounts show small balances and low turnover
c) Government departments and Government-owned companies
d) Finance companies (NBFC except housing finance companies & systematically important NBFC's)
e) Sole proprietorships (i.e., self-employed) where the identity document of both the proprietor and proprietorship are validated online or through other services offered by the issuing authorities.
f) Statutory bodies & Regulators
g) Professionals (whose profession is governed by regulated professional bodies like ICAI, ICSI, ICWAI, Medical Council of India, Bar Council of India, etc.).
h) Manufacturing
i) Self-employed customers with business track record for a reasonable period (at least 3 years)
j) Agriculture / Farming
k) Self – employed individuals / Proprietary Firms / Hindu Undivided Families (HUFs)
l) Government owned companies or its subsidiaries, listed companies or its subsidiaries, reputed multinational companies, regulators and statutory bodies.
m) Partnership Firm with registered deed

Medium & High-Risk Category:

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.

Illustrative examples of medium risk category customers are:

a) Professionals (Eg: Lawyers, CA / CS / Consultants, etc.)
b) Service Provider (Eg: General Industry, Logistics)
c) Companies having close family shareholding where ultimate beneficial ownership is not identifiable
d) Educational trusts (affiliated educational institutions).
e) Limited-liability Partnerships (LLPs).

Few examples of high-risk category customers are:

a) Politically Exposed Persons (PEPs) of Indian/Foreign Origin
b) Non-Resident customers
c) High Net worth Individuals (HNI) (i.e., any person who applies for a loan of an amount of Rs. 1 crore or more), whose identity document is not validated online or through other services offered by the issuing authorities.
d) NGO/NPO
e) Customer name present in Negative List
f) Real Estate Agents/Estate Agents/Real Estate- Builder
g) Trust/Societies(other than Government entities)/Unregulated clubs
h) Multi Level Marketing (MLM)Firms/Chit funds
i) Trading / Wholesaler (Eg: Mining, Minerals, metals, Jewellery, Scrap metal)
j) Firms with sleeping partners.
k) Unlisted companies with unnecessarily complex ownership structure.
l) Person/ Company in business/industry or trading activity where scope or history of unlawful trading/business activity is considered high.
m) Any customer against whom an STR has been filed/ Those with dubious reputation as per public information available

Customers that are likely to pose a higher-than-average risk maybe 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. Enhanced due diligence measures are to be applied based on the risk assessment, thereby requiring intensive due diligence for higher risk customers, especially those for whom the sources of funds are not clear.

The risk categorization criteria referred above are indicative only and a final view would be taken by the Company on a case to case basis. It would be ensured that customer acceptance, identification and risk categorization procedures do not result in unreasonable denial of services to customers, especially to those who are financially or socially disadvantaged. The Company shall keep the risk categorisation of a customer and the specific reasons for such categorisation confidential and shall not reveal this information to the customer to

avoid tipping off.

The risk assessment of customers by the HLF shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the HLF to which power in this regard has been delegated

2. Customer Identification Procedures (CIP) and Identification of Beneficial Owner:

Obtaining Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Procedures (CIP) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the customer relationship. This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions. Identification data that would be required to be obtained for various classes of customers are as below:

Natural Person:

Person who ultimately owns or controls a customer and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

- Address/ location details
- Recent photograph

Legal Persons:

1. Legal status of the legal person/entity through proper and relevant documents.
2. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person/entity is established and verified.

Understand the ownership and control structure of the customer and determine who are natural persons who, ultimately control the legal person. Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc. will be collected for completing the profile of the customer.

3. If the branch/office decides to accept such accounts in terms of the Customer Acceptance Policy, the company should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

Beneficial Owner

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-

i. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b) Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means. Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

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

d) 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.

e) 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.

Declaration Letter from beneficial owner of Entities:

In case of incorporated bodies such as Company, Limited Liability Company, Partnership Firm, Trust, Society, Associations HLF shall identify the beneficial owner of such entities and also obtain a declaration letter in the prescribed format along with certified copies of acceptable OVD documents duly verified and certified by the inspecting officer of HLF with Name, Signature, Employee code, and Office seal.

Know Your Customer Procedure

"Know Your Customer" (KYC) procedure should be the key principle for identification of an individual/corporate for opening an account. The customer identification should entail verification through an employee of the company and on the basis of documents provided by the customer. The objectives of the KYC framework shall be two-fold:

- To ensure appropriate customer identification
- To monitor transactions of a suspicious nature

Branches/offices should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves. Easy means of establishing identity would be documents such as passport, driving license, etc. The Company shall also ensure personal verification by the employee of the company.

Customer Due Diligence (CDD):"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. CDD must be conducted not only at the time of commencement of an account-based relationship but also during the

relationship

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.

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

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non- documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks. The company shall closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) companies.

i) Verification through documents**:**

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company The list such documents are mentioned under the head Acceptable Documents in this policy.

ii) Verification through non-documentary methods**:**

These methods may include, but are not limited to:

(a) Contacting or visiting a customer;
(b) Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
(c) Checking references with other financial institutions; or
(d) Obtaining a financial statement.

iii) Off-line verification through proof of possession of Aadhaar number:

The Company may carry out off-line verification of a customer under the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (Aadhaar Regulations) if the customer is desirous of undergoing Aadhaar off-line verification for identification purpose. No such off-line verification will be performed without obtaining the written consent of the customer in the manner prescribed in the Aadhaar Regulations.

iv) Verification of equivalent e-document:

Where the customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the customer as specified under digital KYC in RBI regulations.

v) Verification through digital KYC:

The Company may carry out verification by capturing live photo of the customer and OVD or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with latitude and longitude of the location where such live photo is being taken by the authorized officer of the Company as prescribed in RBI regulations.

vi) Video based customer identification process (V-CIP):

The Company may undertake live V-CIP for establishment of an account-based relationship with an individual customer after obtaining his informed consent and adhering to the procedures prescribed in RBI regulations. This process shall be treated as face-to-face process for the purpose of customer identification. The liveness check shall not result in exclusion of person with special needs.

vii) Aadhaar based e KYC authentication:

Where the customer submits Aadhaar number the company may carry out authentication of the customers Aadhaar number using e-KYC authentication facility provided by the Unique identification Authority of India (UIDAI). Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by bank official / business correspondents / business facilitators. Further, in such a case, if the customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, the customer may give a self- declaration to that effect and the company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customers profile in order to prevent any fraud

KYC Norms are applicable to all the customers:

- Individuals
- Proprietary concern
- Partnership Firm/ Limited Liability Partnership
- Public Limited Company
- Private Limited Company
- Trust / Society / Association / Club etc.

ACCEPTABLE DOCUMENTS

Individual:

a) the Permanent Account Number or the equivalent e-document thereof or Form 60 as defined in Income-tax Rules, 1962, and

b) the Aadhaar number where, he/ she decides to submit Aadhaar number voluntarily for identification purposes and consents to undergo authentication or proof of possession of Aadhaar number or any Officially Valid Document (OVD-shown below) or the equivalent e-document thereof containing the details of his identity and address

c) any 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 branches/Business Units, to create customer profile for the purpose of risk categorisation and transaction monitoring. Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done by bank official / business correspondents / business facilitators.

List of OVDs:

i. Passport,
ii. the Driving License,
iii. Proof of possession of Aadhaar Number,
iv. the Voter's Identity Card issued by the Election Commission of India,
v. Job Card issued by NREGA duly signed by an officer of the State Government and
vi. Letter issued by the National Population Register containing details of name and address.

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.

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: -

1. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
2. Property or Municipal tax receipt

3. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
4. 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.

Note: A declaration from the customer to be obtained that address will be updated in OVD within 3 months. The customer who has submitted any of the above documents must submit OVD with current address within a period of three months.

Sole Proprietary Firm

At least any two of the listed documents duly verified by the verification officer is mandatory

1. Registration certificate including Udyam Registration Certificate (URC) issued by the Govt
2. Certificate / License issued by municipal authorities under the shop and establishment Act
3. Sale and income tax returns
4. CST / VAT / GST certificate
5. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
6. Complete income tax returns in the name of sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities
7. 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
8. 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
9. Utility bills such as electricity, water, landline telephone bills etc.

Private Ltd Company/Public Ltd Company

1. Certification of Incorporation
2. Memorandum of Association and Article of Association
3. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
4. PAN of the company
5. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company’s behalf.
6. Names of the persons holding senior management position
7. Details of Principle place of business if different from registered office

Other optional Documents

Complete income tax return of the company GST registration or GST returns

Declaration from beneficial owner of the entity

Limited Liability Partnership

1. Certificate of incorporation
2. LLP Deed
3. PAN – Number of Entity
4. Resolution of Partners – certified copy
5. Names of all the partners
6. Details of principal place of business, if it is different from registered office

Other optional documents:

1. Complete income tax return in the name of sole proprietor
2. GST registration and OR GST returns
3. Declaration from beneficial owners of the entity

Partnership Firms:

1. Registration certificate
2. Partnership deed
3. PAN of partnership firm
4. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf Certificate / License issued by municipal authorities under shop and Establishment Act
5. the names of all the partners and
6. address of the registered office, and the principal place of its business, if it is different.

Trust:

1. Registration certificate
2. Trust deed
3. Permanent Account Number or Form No.60 of the trust
4. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
5. The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
6. The address of the registered office of the trust; and
7. List of trustees those discharging the role as trustee and authorised to transact on behalf of the trust

Society:

1. Memorandum of Association and registration
2. Permanent Account Number or Form No.60 of the trust
3. Resolution of the managing body of society
4. Power of Attorney granted to transact on behalf of society

Unincorporated association or body of individuals:

1. Resolution of the managing body of such association or body of individuals
2. Power of attorney granted to him to transact on its behalf
3. An officially valid document in respect of the person holding an attorney to transact on its behalf.
4. Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals
5. PAN or Form No. 60 of the unincorporated association or a body of individuals

Registration with DARPAN portal

HLF shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If such customers are not registered, HLF shall register the details on the DARPAN Portal. HLF shall also maintain such registration records for a period of five years after the business relationship between the customer and the HLF has ended or the account has been closed, whichever is later.

Non-Profit Organization is an entity constituted for religious or charitable purpose referred to Clause 15 of Sec 2 of income Tax Act 1962

A. Customer profile Verification

The company while evaluating a prospective customer obtains important information like the customer's source of funds, source of income and assets, etc. through collection of following details:

(a) Details of employment/ business/ vocation or profession
(b) Details of income and annual income
(c) Details of assets owned, such as house, vehicle, etc.
(d) Other personal details such as qualification, marital status
(e) Dealings with banks/ other financial institutions and the credit history

Drawing up of customer profile would give an idea as to the nature and volume of transactions/activities to expect in the account as assessed/ envisaged at the time of opening of an account. If the transactions are in variance with the profile of client, the customer should be contacted for further details to the satisfaction of the company.

B. Reliance on third party due diligence:

For the purpose of identifying and verifying the identity of customers 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, the Company may rely on a third party; subject to the condition that:

i. the Company obtains necessary information of such client due diligence carried out by the third party;
ii. the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
iii. the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PMLA Act;
iv. the third party is not based in a country or jurisdiction assessed as high risk; and
v. the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.
vi. 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.

C. Resolution of Discrepancies:

HLF business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

D. Periodic updation of KYC of Customers

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

The Company shall have a system in place for periodical updating of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low-risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers.

HLF 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.

Updating of Legal Entities on to CKYC Portal

HLF shall upload the KYC data pertaining to accounts of Legal Entities (LE) opened on or after April 1, 2021, on to CKYCR in terms of Rule 9 (1A) of the PML Rules. HLF shall also ensure that in case of accounts of LEs

opened prior to April 1, 2021, the KYC records are uploaded on to CKYCR

KYC documents are to be updated periodically for all the customers with outstanding liability with HLF. Frequency of up dation is given below:

Low Risk	Not less than once in 10 years
Medium Risk	Not less than once 8 years
High Risk	Not less than once 2 years

In respect of an individual customer who is categorized as low risk, HLF shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. HLF shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

Updating / Periodic Updating of KYC:

The procedure for updating the KYC Documents is given below. HLF staff has to ensure the updating of KYC as per the above frequency. In order to ensure customer convenience, the HLF considers making available the facility of updation / periodic updation of KYC at any branch

a) Individuals:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the RE, customer's mobile number registered with the HLF, letter, etc.

ii. **Change in address**: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the RE, customer's mobile number registered with the HLF, 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.

Customers other than individuals:

No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the HLF, letter from an official authorized by the LE in this regard, board resolution, etc.

Further, HLFs 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, HLF shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer. Further, in case the validity of the CDD documents available with the HLF has expired at the time of periodic updating of KYC, HLF shall undertake

the KYC process equivalent to that applicable for on-boarding a new customer. ii. Customer's PAN details, if available with the HLF

Due Notices for Periodic Updation of KYC

HLF shall inform customers in advance to update their KYC, with multiple reminders before and after the due date, including at least one by letter. All communications must be recorded for audit purposes. A detailed communication and escalation process shall be outlined in the internal process note and implemented by January 1, 2026.

E. Internal Risk Assessment

In line with the RBI Circular No. RBI/DOR/2025-26/361 DOR.AML.REC.No.280/14.01.003/2025-26 dated 28th November, 2025 the Company shall have a Risk Based Approach (RBA) for mitigation and management of the identified risk along with controls and procedures.

F. Photographs:

At the time of evaluating the proposal, two passport size photographs of each borrower and guarantor should be obtained which are self-attested.[1] Where the borrower and/or guarantor are an artificial person, photographs of directors/ partners/ Karta as the case may be, need to be obtained which are self-attested.

G. Field Inspection:

As part of proposal evaluation process, an employee of the company visits the office and/or residential address of the customer to verify the claims made in the loan application form and meets the borrower to address doubts, if any.

H. Enhanced due diligence

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced

scrutiny.

EDD includes:

a. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;

b. Checking references with other financial institutions;

c. Obtaining a bank statement of Accounts / Financial statement

The Company shall also undertake enhanced due diligence in case of non-face-to-face onboarding facilities (such as CKYCR, Digi Locker, equivalent e-document, etc.) for establishing the relationship with the customer without meeting the customer

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorization of risk, up dation of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

3. Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. The branch/office may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions, which exceed these limits. High-risk accounts have to be subjected to intensify monitoring. The company should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

Branches are required to record and report all transactions of suspicious nature in deposit, loan and remittance accounts etc, with full details to their controlling Offices. The principal officer/Officer -in charge, vested with the authority to open the account, is to ensure compliance with the KYC guidelines. The employee/officer, who has interviewed the customers to subscribe his signature for having interviewed the prospective customer and the officer before permitting opening of the account, to satisfy that all aspects of KYC guidelines are complied with.

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

Reporting of Suspicious Transactions:

To observe four eyes concept in reporting suspicious transactions at branch level, first dealing officer at the branch will report to the Branch Manager (BM), who will get himself satisfied about existence of a suspicious activity/nature and then report to the controlling office. Further course of action is to be recommended by the controlling officer in consultation with Law Department to H.O. The designated officer at H.O has to take up the matter with appropriate law enforcing authorities designated under the relevant laws governing such activities.

"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.

e. 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.

(i) Cash Transactions

In line with the Finance Act 2017, the maximum amount of Cash that can be collected from the customer should not exceed an amount of Rs. 1,99, 999.The amount of Rs.1,99,999 will be the total amount that can be collected against all the contracts of a customer put together in a month.

Reporting Requirement to Financial Intelligence Unit of India:

While furnishing information to the Director, FIU-IND, HLF will abide by the time specification as stipulated by FIU and also shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

HLF shall file the STR reports on FINGATE 2.0 only through competent Authority. Any suspicious transaction concluded by the reporting authority shall be reported to FIU immediately and all records of transaction and analysis is kept confidential. To identify and report suspicious transactions effectively, the company shall implement robust software that generates alerts when transactions are inconsistent with a customer's risk categorisation and updated profile.

HLF directors, officers, and all employees shall ensure that the fact of maintenance of records 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

(ii) Terrorist Finance:

In case the name of any banned organization is noticed as payee/endorsee/applicant, the first dealing officer shall report the same to the Principal Officer. Reporting of such transactions as and when detected is to be done as under:

Reporting by	**Reporting to**
Branch	Controlling Office
Controlling office	Principal Officer (PO)/H.O
PO/H.O	FIU-IND

All cash transactions, where forged or counterfeit Indian currency notes have been used, shall also be reported immediately by the branches, by way of Counterfeit Currency Reports (CCRs) to the Principal Officer, through proper channel, for onward reporting to FIU-IND.

HLF shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries circulated by Reserve Bank of India from time to time, and publicly available information under FATF (Financial Action Task Force)

Compliance of procedure under Sec 12 A of Weapons of Mass Destruction (WMD)

(a) All offices 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 (Annexure III of Master Direction of RBI last updated upto 17.10.2023).

(b) In accordance with paragraph 3 of the aforementioned Order, all offices 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, all offices 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, the transaction details with full particulars of the funds, financial assets or economic resources involved, be immediately reported to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

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

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

4. Risk Management

For risk management, the company shall have a risk-based approach which includes the following.

The company shall categorise customers into low, medium, and high-risk categories, based on its assessment and risk perception

The company may lay down broad principles for the risk-categorisation of customers.

The company shall undertake risk categorisation based on parameters such as the customer's identity, social / financial status, nature of business activity, and information about the customer's business and its location, geographical risk covering customers as well as transactions, type of products / services offered, delivery channel used for delivery of products / services, types of transactions undertaken such as cash, cheque / monetary instruments, wire transfers, forex transactions, etc. The company may also factor in the ability to confirm identity documents through online or other services offered by issuing authorities, while considering customer's identity.

The company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements. It would be ensured that the audit machinery is staffed adequately with individuals who are well

versed in such policies and procedures. Chief Compliance Officer (CCO) is the principal officer for monitoring Anti Money Laundering Issues. A dedicated credit audit team under the direct supervision of Head - Credit checks and confirms compliance with the KYC policies and procedures in respect of all the loan contracts. Internal audit system to verify compliance with KYC / AML policies and procedures.

5. Training Program:

As part of induction process, employees across the country are trained in KYC guidelines through online training module. Updating and modifications, if any, in the guidelines are also cascaded to the entire team to keep them abreast of the changes

6. Internal Credit controls and Internal Audit:

Chief Compliance Officer is the nodal officer for monitoring Anti Money Laundering issues like review of transactions of suspicious nature and verifying compliance of guidelines in this regard. KYC/AML guidelines are inbuilt into the Standard Operating Procedure by designating a maker checker & reviewer

for each activity. The location in charge / executive verifies the original document of the borrower and endorses "Original Seen and Verified" in every document. The Hub Credit Administrator (HCA) checks and confirms if the above documents are in place before the disbursal of the loan. The Credit Quality Compliance team at RMC reviews the entire file. The Company shall ensure compliance with KYC Policy through internal audit system to verify the compliance with KYC/AML policies and procedures and submission of quarterly audit notes and compliance to the Audit Committee.

7. Record Keeping:

As per the guidelines of Reserve Bank of India, the company is required to prepare and maintain documentation on their customer relationships and transactions to meet the requirements of relevant laws and regulations and to enable any transactions effected through them to be reconstructed.

All financial transactions records, relevant customer identification and KYC records are required to be retained for 10 years after the transaction has taken place and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

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

a. maintain all necessary records of transactions between the company and the customer, both domestic and international, for at least five years from the date of transaction;
b. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

c. make available swiftly, the identification records and transaction data to the competent authorities upon request;
d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
e. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
    i. the nature of the transactions;
    ii. the amount of the transaction and the currency in which it was denominated;
    iii. the date on which the transaction was conducted; and
    iv. the parties to the transaction.
f. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
g. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

8. Assessment and review:

The Company shall also undertake periodic (at least annual) assessment of KYC/AML policies and procedures to ensure that compliance functions continue to function effectively.

9. Introduction of new technologies:

HLF shall identify and assess the Money Laundering (ML) / Terror Financing (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, HLF 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.

Secrecy Obligations and Sharing of Information:

a) The company shall maintain secrecy regarding the customer information that arises out of the contractual relationship between the company and the customer.
b) The company shall treat information collected from customers for the purpose of opening of account as confidential and shall not divulge details thereof 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, the NBFC shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
d) The exceptions to the said rule shall be as under:
    i. Where disclosure is under compulsion of law,
    ii. Where there is a duty to the public to disclose,
    iii. Where the interest of the company requires disclosure, and

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

Money Laundering and Terrorist Financing Risk Assessment:

a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercises 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.
b) 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, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator / supervisor may share with the company from time to time.
c) The company shall properly document its risk assessment and it shall be proportionate to the nature, size, geographical presence, complexity of activities / structure, etc. of the company. The company shall review it at least annually.
d) The NBFC shall present the outcome of the exercise to the Board or any committee of the Board to which the Board has delegated power in this regard. The outcome shall also be made available to competent authorities and self-regulating bodies.

10. Principal / Nodal Officer:

Principal Officer of HLF shall be appointed by the Board at Management Level only. Principal officer for HLF is Chief Compliance Officer. The Company shall communicate the name, designation, address and contact details of the Principal officer and Designated Director to the FIU-IND and RBI.

Chief Compliance Officer

Hinduja Leyland Finance Limited No. 27A, Developed Industrial Estate Guindy, Chennai - 600032

Phone: +91 44 22427526

Email: cco@hindujaleylandfinance.com

11. Designated Director:

The Board at its meeting held on September, 2023 had nominated Mr. Sachin Pillai, Managing Director and Chief Executive Officer as the designated director to ensure overall compliance with the obligations imposed by KYC policy and the PML act. The company shall not nominate the Principal Officer as the 'Designated Director'.

This policy was last reviewed and approved by the Board on 20th May,2026.