



ASK Financial Holdings Private Limited

Know Your Customer (KYC), Anti Money Laundering  
(AML),  
Combating Financing of Terrorism (CFT) and  
Customer Acceptance Policy (CAP)

Version 7.0

February 2026

Document review and revision history

| Version | Department                                    | Author   | Date          | Revision                                     |
|---------|---|--|---------------|--|
| 1.0     |   | Frederick Pinto                                    | 16-11-2017    | Formulation of New Policy                    |
| 2.0     |   | Lijo Varghese                                      | 23-06-2020    | Review                                       |
| 3.0     | Credit and Risk                               | Dhruva Shah  | 05-06-2024    | Annual Updation                              |
| 4.0     | Compliance                                    | Simit Mehta  | 12-11-2024    | Policy Updation                              |
| 5.0     | Compliance                                    | Simit Mehta  | 08-07-2025    | Policy Updation as per regulatory update     |
| 6.0     | Compliance                                    | Simit Mehta  | 04-11-2025    | Policy Updation as per regulatory guidelines |
| 7.0     | Compliance and Credit and Risk and Operations | Ketaki Sawant and Dhruva Shah and Shrutika Jaguste | Board Meeting | Policy Updation as per regulatory guidelines |

Contents

|   |    |
|---|----|
| 1. Preamble:.....   | 4  |
| 2. Objectives of the Policy .....   | 4  |
| 3. Purpose of the policy:.....  | 4  |
| 4. Compliance with KYC Policy .....   | 5  |
| 5. What is Money Laundering .....   | 5  |
| 6. Customer Acceptance Policy .....   | 6  |
| 7. Customer Identification Procedures .....   | 7  |
| 9. Maintenance of records of transactions / Information to be preserved / Maintenance and preservation of records / Cash and STR to FIU-IND ..... | 14 |
| 10. Risk Management .....   | 17 |
| 11. Employee Due Diligence and Training Program .....   | 18 |
| 12. Background Search.....  | 18 |
| 13. Confidentiality of Customers data: .....  | 18 |
| 14. Internal Control System:.....   | 18 |
| 15. Principal Officer and Designated Director .....   | 19 |
| 16. General.....  | 19 |
| 17. Review of this Policy .....   | 20 |

1. Preamble:

- A. ASK Financial Holdings Private Limited (hereinafter referred to as a 'Company' or 'ASK Finance) is a Base layer Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India ('RBI').
- B. RBI vide its Master Direction – Know Your Customer (KYC) Directions dated February 25, 2016 (hereinafter referred to as “KYC Master Directions”) and as updated from time to time has issued comprehensive guidelines on KYC norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures are formulated and put in place with the approval of the Board. Additionally, the Company is required to comply with The Prevention of Money Laundering Act, 2002 (hereinafter referred to as 'Act' or 'PML Act'), The Prevention of Money-Laundering (Maintenance of Records Rules), 2005 (hereinafter referred to as 'Rules' or 'PML Rules'), Unlawful Activities (Prevention) Act, 1957 (hereinafter referred to as 'UAPA') as updated from time to time.
- C. The objective of PML Rules is to prevent NBFCs from being used, intentionally or unintentionally by criminal elements for money laundering activities. Further, the KYC Master Directions requires all regulated entities to determine the identity and beneficial ownership of accounts maintained by it, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc.
- D. To comply with the laws and regulations mentioned above, the Company has adopted this Policy on KYC, AML, CFT and Customer Acceptance, hereinafter referred to as Know Your Customer ('KYC'), Anti Money Laundering ('AML'), Combating Financing of Terrorism ('CFT') and Customer Acceptance Policy (CAP) or “Policy”. This policy must be read in conjunction with the RBI's KYC Master Directions. The main objective of this policy is to provide mechanism for undertaking appropriate and satisfactory diligence of the customers and identification of their beneficial owners and ensure compliance with the specific obligations and reporting requirements as provided under the KYC Master Directions.
- E. As per RBI's Amendment to Master Direction (MD) on KYC bearing reference no. DOR.AML.BC.No.66/14.01.001/2019-20 dated April 20, 2020, wherein the RBI has inserted a new clause (5A) to chapter II of Master Direction - Know Your Customer (KYC) Direction, 2016 requiring regulated entities to carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels.
- F. Chapter V of RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 and RBI (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025.
- G. All provisions in the Policy as applicable for NBFC – Middle Layer shall be effective within 90 days after the Company crosses the threshold for Middle Layer.

2. Objectives of the Policy

- A. The objectives of the Policy are:
  - a. to enable the Company to have the positive and complete identification of its customers;
  - b. to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities;
  - c. to comply with all the legal and regulatory obligations in respect of KYC, AML and CFT measures and obligation of the Company under the PML Act, PML Rules, RBI's NBFC Master Directions including KYC Master Directions;
  - d. to establish a proper Customer Due Diligence process before on-boarding Customers; and
  - e. to monitor, maintain and report all suspicious transactions.
- B. In accordance with this Policy, Company undertakes to use reasonable efforts to ensure that none of its people or associates are used to provide support to individuals or entities associated with terrorism.
- C. This policy shall be read in with any relevant and applicable policy / procedures may be adopted by ASK Investment Managers Limited, the ultimate holding company of Company, and Company shall be bound by the stricter norms envisaged under the aforesaid policy / procedure.
- D. This Policy of the Company provides for sufficient framework to cover all the risk assessment parameters for mitigating its money laundering and terrorist financing risks and to ensure that all existing accounts of the Company are compliant with the updated Policy of the Company at all times.
- E. All Customer's accounts shall be subject to review from time to time as per the updated Policy of the Company.

3. Purpose of the policy:

- A. The purpose of this policy is to put in place process and procedures including systems, if any, to help control financial

frauds, identify money laundering and suspicious activities and safeguarding the company from being used for transfer or deposit of funds derived from criminal activity or for financing of terrorism.

- B. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. Thus, this KYC policy has been framed by the Company for the following purposes:
- a. To prevent criminal elements from using Company for money laundering activities.
  - b. To enable Company to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
  - c. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
  - d. To comply with applicable requirements of (i) the Know Your Customer and Anti-Money Laundering Laws; (ii) Sanctions and (iii) all other applicable export control, anti-boycott and sanctions laws relating to its business and facilities. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

This Policy has following key elements:

- i. Customer Acceptance Policy (CAP);
- ii. Customer Identification Procedures (CIP);
- iii. Monitoring of Transactions;
- iv. Risk management; and
- v. Employee Due Diligence

#### 4. Compliance with KYC Policy

For the purpose of compliance with KYC Policy and as required under the KYC Master Directions, the Company has additionally approved the following:

- A. The ‘Senior Management’ of the Company for the purpose of implementation and compliance of this KYC Policy and KYC Master Directions would mean the Board of Directors, Designated Director, Principal Officer, Compliance Officer, Chief Financial Officer and head of each department.
- B. The responsibility for effective implementation of this KYC Policy and procedures provided herein shall be with the Operations department.
- C. The Company has appointed external auditors to undertake internal audit to verify the compliance with KYC/AML policies and procedures.
- D. The Company will ensure submission of quarterly audit notes and compliance to the Credit & Risk Management Committee (RMC).
- E. The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced at any point of time.
- F. Separate process notes may be made for implementation of this policy, as maybe be applicable from time to time, with the approval of the MD & CEO

#### 5. What is Money Laundering

- A. Money Laundering (ML) is the process by which persons with criminal intent or persons involved in criminal activity attempt to hide or disguise the true origin and ownership of the proceeds of their criminal activities by routing through / use of the financial system so that after a series of transactions, the money, its ownership and the income earned from it appear to be legitimate, thereby avoiding prosecution, or conviction for such activities. This is often achieved by converting the original illegally obtained proceeds, usually in cash, into other forms like deposits/securities and by transferring them from one financial institution to another using accounts of apparently different persons or businesses.
- B. Section 3 of the PML Act defines offence of ML in following words: “Whosoever 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 including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering”.
- C. Money Laundering Risks
  - a. Reputation Risk- Risk of loss due to severe impact on Company’s reputation. This is of particular concern given the nature of the Company’s business, which requires maintaining the confidence of investors, creditors and the general marketplace.

- b. Compliance Risk- Risk of loss due to failure of compliance with key Regulations.
- c. Operational Risk- Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.
- d. Legal Risk- Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with Law and having a negative legal impact on. Specific negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.
- e. Financial Risk- Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact.

#### 6. Customer Acceptance Policy

- A. For the purpose of Company's KYC policy a 'Customer' means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- B. Further, a "Walk-in Customer" means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.
- C. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Company or meeting the officials of Company.
- D. The term "Person" shall have the meaning given to it under the KYC Master Directions of RBI, as may be amended from time to time, read with the Act which at present includes individual, a Hindu undivided family, a company, a trust, a firm, an association of persons or body of individuals (whether incorporated or not), every artificial, juridical person not falling within any one of the above persons, and any agency, office or branch owned or controlled by any one of the persons.
- E. Company's Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers which broadly includes the following:
  - a. The Customer must be a citizen and resident of India.
  - b. No account will be opened in anonymous or fictitious / benami name(s) / entity(ies).
  - c. No transaction or account-based relationship is undertaken without following the Customer Due Diligence ("CDD") procedure.
  - d. Customers will be accepted only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before opening a new account are to be ensured so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc., or with persons whose name appears in the sanctions lists released and updated by the RBI from time to time.
  - e. Customers shall be classified into various risk categories and based on risk perception, the acceptance criteria for each category of customers will be applied. Parameters of risk perception are clearly defined in terms of nature of business activity, location of customer and its clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk. Customer requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs – as explained in Annexure I) may, if considered necessary, will be kept in the High Risk Category.
  - f. For the purpose of risk categorization of customer, the Company shall obtain the relevant information from the customer at the time of account opening.
  - g. ASK permits customer onboarding through face-to-face, video-based Customer Identification Process (V-CIP), and non-face-to-face digital channels in line with RBI's updated KYC provisions. Digital and non-face-to-face onboarding shall be subject to additional risk controls, including liveness checks, document authenticity verification, and multi-factor
  - h. Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Act read with Rules and RBI guidelines / instructions.
  - i. Not to open an account or close an existing account where the company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and / or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the company. It may, however, be necessary to have suitable built-in safeguards to avoid harassment of the customer. 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. The Company shall consider filing a Suspicious Transaction Report (STR), if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer. No KYC application for onboarding or periodic updates shall be rejected without proper application of mind. Officers must record detailed reasons for rejecting any application ensuring decisions are fair and accountable.

- j. Circumstances, in which a customer is permitted to act on behalf of another person/entity, would be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.
- k. Customer Due Diligence (CDD) procedure shall be applied at the Unique Customer Identification Code (UCIC) level enabling seamless monitoring across all services. -
- l. Any mandatory information to be sought for KYC purpose while (i) giving effect to the transaction effected through the Company and (ii) during the periodic updation of the same, shall be clearly specified.
- m. Any optional and/or additional information shall be sought separately with consent, clearly indicating that providing of such information is optional.
- n. In case Permanent Account Number (“PAN”) of the Customers are obtained, the same shall be verified from the verification facility of the issuing authority.
- o. In case an equivalent e-document is obtained from the Customers, the digital signature affixed on such e-document shall be verified as per the provisions of the Information Technology Act, 2000 and the Company shall collect live photo of the Customer in the prescribed manner.
- p. The Company will not discriminate the Customers based on their religion, caste, sex, color, financial or social characteristics.
- q. Documentation requirements and other information will be collected in respect of different categories of the Customers and keeping in mind the requirements of Act and the guidelines issued by RBI and other statutory and regulatory bodies from time to time.
- r. The profiles of the Customers will be treated as a confidential and details contained therein will not be divulged to outsiders for any purposes other than as mutually agreed with the relevant Customer or as may be required to be shared with any regulatory body or agency or to service providers with whom the company has entered into agreement for the purpose of meeting the objective as agreed with the customer.
- s. The responsibility of ensuring compliance in relation to the Customer Acceptance Policy (“CAP”) shall be with the Board.
- t. The Company shall not grant any loan where the Company is unable to apply appropriate customer identification / due diligence measures due to any of the following circumstances:
  - i. The Company is unable to verify the identity of the customer;
  - ii. The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
  - iii. Identity of the customer directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Government of India, State Governments or any other national or international body / organization.
- u. Where an existing customer has already undergone KYC with ASKFH, no fresh CDD shall be performed for subsequent account relationships, provided there is no material change in the customer’s risk profile or ownership structure.

## 7. Customer Identification Procedures

- A. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer along with brief details of their beneficial owners, wherever applicable, whether regular or occasional and the purpose of the intended nature of Business relationship.

- B. 'Being satisfied' means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers.
- C. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). For customers that are natural persons, Company shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall -
- a. verify the legal status of the legal person/ entity through proper and relevant documents;
  - b. verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person;
  - c. understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.
- Customer identification requirements in light of the provisions of KYC Master Directions read with Act and Rules issued in this respect are indicated in Annexure I. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure II.
- D. This policy shall be referred at all stages of the customer journey with the Company. Accordingly, the identification procedure will be carried out at different stages of customer journey, i.e. while establishing a relationship; carrying out a financial transaction or when there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
- E. As per Rule 9(IA) of the Prevention of Money Laundering Rules, 2005, Company is required to identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client 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. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:
- a. Where the client is a Company, Company shall identify its beneficial owners as natural person(s) who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.  
Explanation- For the purpose of above -
    - i. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company- 'Control' includes right to appoint majority of directors or control management/policy decisions  
- Where no natural person meets the 10% threshold, identify person exercising control through other means or the senior managing official.
    - 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.
    - iii. If no natural person meets the 10% threshold, ASKFH shall identify the person exercising control through other means or the senior managing official.
  - b. Where the client is a Partnership Firm, Company shall identify its beneficial owners as 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 above, "control" shall include the right to control the management or policy decision.
  - c. Where the client is an Unincorporated Association or Body of Individuals, Company shall identify its beneficial owner as the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.  
Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner shall be the relevant natural person who holds the position of senior managing official.

- d. Where the client 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. and beneficiaries with 10% or more interest in the trust shall be identified as per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025.
- e. For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub rule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:
  - f. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
  - g. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.
- F. Documentation requirements and other information from the customers shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002 and guidelines issued by RBI from time to time.
- G. Necessary checks wherever and to the extent possible, shall be conducted before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities.
- H. The Company will also carry out an independent research on concerned entities through publicly available information, as necessary. In case of any gaps in the information and documents available, enhanced due diligence will be conducted and a report will be submitted to Compliance Officer/senior management personnel of the Company for their approval.
- I. The Company will specifically comply with the norms prescribed under the KYC Master Directions before onboarding and serving a customer who is a Politically Exposed Person (PEP), Professional Intermediaries, Self Help Groups (SHGs), Foreign Students, customers from jurisdiction that do not or insufficiently apply the Financial Action Task Force (FATF) recommendations or such other person as expressly provided therein.
- J. Reliance on Customer Due Diligence done by a third party
 

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on customer due diligence done by a third party, subject to the following conditions:

  - a. Records or the information of the customer due diligence carried out by the third party is obtained during normal course of business from the third party or from the Central KYC Records Registry.
  - b. The Company will satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
  - c. The third party shall not be based in a country or jurisdiction assessed as high risk.
  - d. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.
- K. Ongoing Due Diligence
  - a. The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth. Following types of transactions shall necessarily be monitored by the Company:
 

Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose. PAN shall be mandatory for all monetary transactions

    - i. Transactions which exceed the thresholds prescribed for specific categories of accounts.

- ii. High account turnover inconsistent with the size of the balance maintained.  
The extent of monitoring shall be aligned with the risk category of the customer.
- b. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
- c. The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored. [Reference: Chapter VI of RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 - Multiple small cash deposits across the country in one account and large number of cheques bearing similar amounts/dates shall be immediately reported to RBI and FIU-IND.]
- d. Where multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

L. Updation / Periodic Updation of KYC

- a. The documentation requirements would be reviewed periodically and updated keeping in view emerging business requirements. The Company shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least:
  - i. once in two years for high-risk customers; As per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 - Advance Intimation Requirements:
    - At least THREE advance intimations including at least ONE by letter at appropriate intervals prior to KYC due date
    - Intimations shall include: (a) due date; (b) documents/information required; (c) channels available for updation; (d) escalation mechanism for seeking help; (e) consequences of failure to update
    - Issue of advance intimation/reminder shall be duly recorded in Company's system against each customer for audit trail.
  - ii. once in three years for medium risk customers; and
  - iii. once in five years for low-risk customers from the date of opening of the account / last KYC updation.
  - iv. As per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, every Low-risk individual customers have up to ONE YEAR from KYC falling due or up to June 30, 2026, whichever is later, to complete periodic updation. The accounts of such customers shall be subject to regular monitoring.
- b. The periodic updation process in this regard would follow as under:

Customers shall be categorized into Low/Medium/High Risk as mentioned below:

| Low Risk  | Medium Risk  | High Risk  |
|---|--|--|
| Domestic Listed Companies and their subsidiaries/entities in which they have majority stake | Below entities if not involved in High-Risk Business | Others not covered in low and Medium Risk categories, Including: |
| Public Sector Companies   | Registered Partnership firms                         | Politically Exposed Person                                       |
| Regulated Financial Entities  | Limited Liability Partnership Firms                  | Individual with CIBIL Score between 650 to 675                   |
| Individual with Score more than 700   | Unlisted Private/Public Limited Companies            | Proprietorship Firms   |
|   | Registered Trust                                     | Unregistered Partnership Firms                                   |
|   | Unregistered Trust for Securitization Transaction    | AOP/BOI  |
|   | Individual with CIBIL Score between 675 to 700       | Unregistered Trust (except for PTC Transaction)                  |
|   |  | NON-Profit Organizations   |

|  |  |   |
|--|--|---|
|  |  | All Stressed Accounts (SMA 1 and above)   |
|  |  | Entities in Below Business<br>1. Virtual Currency/ Chit Funds.<br>2. Gems & Jewellery/Bullion |

The Company shall conduct ML/TF Risk Assessment exercise at least annually, The outcome of Risk Assessment shall be put up to the BOARD for review and approvalAs per Chapter II of RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025,the ML/TF Risk Assessment shall cover clients, countries/geographic areas, products, services, transactions, and delivery channels with a periodic review of risk categorization shall be conducted at least once in six months.

i. Individuals:

- No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer’s email-id registered with the Company, customer’s mobile number registered with the Company, digital channels (such as mobile application of Company), letter, etc.
- Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer’s email-id registered with the Company, customer’s mobile number registered with the Company, digital channels (such as mobile application of Company), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

Further, the Company at its option, may obtain a copy of Officially Valid Document (‘OVD’) or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of the KYC Master Directions, for the purpose of proof of address, declared by the customer at the time of periodic updation. Accounts of customers, who were minor at the time of opening account, on their becoming major: In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Company. Wherever required, the Company may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.

- Aadhaar OTP based e-KYC in non-face-to-face mode may be used for periodic updation. For low-risk customers with no changes in their KYC information, a self-declaration may also be permitted as per the latest guidelines. Additionally, Regulated Entities can now utilize Business Correspondents to assist with the KYC updating process. However, the general guidelines for KYC periodic updation as outlined in the Master Directions will continue to apply unless specifically relaxed under the amended regulations.
- Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with it in the customer’s profile, in order to prevent any fraud.
- The company will make reasonable efforts to reach out customers (depending upon their risk profile and frequency for updating of KYC records) seeking their updated status / documents for any change in KYC through their registered email address, registered mobile number and in case the emails are undelivered will reach out to their registered address through registered post. If the customer remains incommunicado despite of reasonable efforts to reach out to their registered address / registered email id, the company will continue maintain the existing KYC records as the most updated one.

ii. Customers other than individuals:

- No change in KYC information: In case of no change in the KYC information of the Legal Entity (‘LE’) customer, a self-declaration in this regard shall be obtained from the LE customer through their email id registered with the Company, digital channels (such as mobile application of Company), letter from an official authorized by the LE in this regard, board resolution, etc. Further, the Company shall ensure during this process that Beneficial Ownership (BO) information available with us 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, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new LE customer. The company will make reasonable efforts to reach out customers (depending upon their risk profile and frequency for updating of KYC records) seeking their updated status / documents for any change in KYC through their registered email address, registered mobile number and in case the emails are undelivered will reach out to their registered address through registered post. If the customer remains incommunicado despite of reasonable efforts to reach out to their registered address / registered email id, the company will continue maintain the existing KYC records as the most updated one.
- iii. Additional measures: In addition to the above, the Company shall ensure that,
- The KYC documents of the customer as per the current Customer Due Diligence ('CDD') standards are available with us. This will be applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, it will undertake the KYC process equivalent to that applicable for on-boarding a new customer.
  - Customer's PAN details, if available with us shall be verified from the database of the issuing authority at the time of periodic updation of KYC.
  - Acknowledgment shall be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the REs and an intimation, mentioning the date of updation of KYC details, shall be provided to the customer.
  - In order to ensure customer convenience, the Company may make available the facility of periodic updation of KYC at any branch, in line with this policy.
- iv. In order to comply with the PML Rules, the customers of the Company shall be obligated to report any changes in the documents submitted earlier at the time of establishment of business relationship / account- based relationship and thereafter, within 30 days of such update alongwith relevant documents for the purpose of updating the records maintained by the Company.
- In case of existing customers, the Company shall mandatorily obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which the Company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.
  - Provided that before temporarily ceasing operations for an account, the Company shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, the Company may provide appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.
  - Provided further that if a customer having an existing account-based relationship with the Company gives in writing that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No. 60, the Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.
  - Explanation – For the purpose of the above clause, “temporary ceasing of operations” in relation to an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Company till such time the customer complies with the above provisions. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.
  - Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance. It is reiterated that the Customer Identification Procedure will be carried out at the following stages:
    - while establishing a business relationship; or

- carrying out a financial transaction; or
- where the company has a doubt about the authenticity/veracity; or
- inadequacy of the previously obtained customer identification data if any; or
- when the company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

No deviations or exemptions shall normally be permitted. In case of extreme cases of exceptions, concurrence of CEO should be obtained duly recording the reasons for the same.

M. Customer Onboarding / Due Diligence process-

- a. The customer makes the request for loan through the help of the representative of Company and shares the copies of KYC documents.
- b. The PAN card of the customer is verified through the PAN verification facility of National Securities Depositories Limited ('NSDL').
- c. The back office team verifies the KYC documents and in case where the images provided by the Customer is not from the original KYC documents, but of the photocopy of the KYC documents, the loan application / KYC is rejected by the back office team.
- d. The back-office team ensures that the photograph of the Customer matches with the PAN/ Aadhar Card of the customer.
- e. On successful completion of the test, the customer is onboarded in the system for processing of loan request and issuance of sanction letter.

8. Monitoring And Reporting of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the account. Company shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified. The Company will undertake following steps for effecting monitoring of transactions:

A. Monitoring of transactions in order to identify unusual behaviour

- a. Company will prescribe internal threshold limits for a particular categories of accounts which may be prone to be used for prohibited activities and pay particular attention to the transactions which exceed those limits.
- b. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall be periodically monitored.
- c. All complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose will be thoroughly reviewed.
- d. As per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, any single transaction or multiple connected transactions equal to or exceeding ₹50,000 shall require mandatory KYC verification (occasional transactions). All international money transfer operations shall be monitored regardless of amount.
- e. Upon identification of any unusual behavior, enhanced due diligence will be undertaken.
- f. Periodic review of manner of assessment of Suspicious Transactions will be undertaken.
- g. Based on the results of such enhanced due diligence, suspicious transactions identified if any shall be reported to relevant internal teams, third parties and regulators as required by the applicable laws.

B. Periodic Review of Risk Categorization of customers

- a. Company shall carry out the periodic review of risk categorization of transactions/customer's accounts and the need for applying enhanced due diligence measures at a periodicity of not less than once in twelve months.
- b. Periodic review of risk categorization of the Customers i.e. as and when a Customer moves from a lower risk category to higher risk category shall be undertaken as per this Policy;
- c. Higher risk accounts shall be subjected to intense monitoring.
- d. Company shall set key indicators for such accounts basis the background of the customer, country of origin,

sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring; and

- e. Company shall also explore the possibility of validating the new account opening applications with various watch lists available in public domain, including RBI watch list and sanctions list.

9. Maintenance of records of transactions / Information to be preserved / Maintenance and preservation of records / Cash and STR to FIU-IND

A. Maintenance of records of transactions:

The Company shall maintain proper record of the transactions as required under Section 12 of the Act read with Rules 3 of the Rules as mentioned below:

- a. All cash transactions of the value of more than Rs. 10 lakhs (Indian Rupees Ten Lakhs Only) or its equivalent in foreign currency, though by policy the Company does not accept cash deposits in foreign currency.
- b. All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs (Indian Rupees Ten Lakhs Only) or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate value of such transactions exceeds Rs 10 lakhs (Indian Rupees Ten Lakhs Only) or its equivalent in foreign currency;
- c. All transactions involving receipts by non-profit organizations of Rs. 10 lakhs or its equivalent in foreign currency.
- d. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
- e. KYC documents, transaction data, and STRs shall be retained for a minimum period of five (5) years after the business relationship has ended or the transaction is completed, whichever is later.
- f. All suspicious transactions whether or not made in cash and by way of any of the modes as under:
  - i. deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to any currency maintained by way of:
  - ii. cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
  - iii. travellers cheques, or transfer from one account within the same financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or any other mode in whatsoever name it is referred to;
  - iv. credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the financial institution and intermediary, as the case may be;
  - v. money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-
    - payment orders, or
    - cashiers cheques, or
    - demand drafts, or
    - telegraphic or wire transfers or electronic remittances or transfers, or
    - internet transfers, or
    - Automated Clearing House remittances, or
    - lock box driven transfers or remittances, or
    - remittances for credit or loading to electronic cards, or
    - any other mode of money transfer by whatsoever name it is called;
  - vi. loans and advances including credit or loan substitutes, investments and contingent liability by way of:
    - subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, inter-bank participation or any other investments in securities or the like in whatever form and name it is referred to, or
    - purchase and negotiation of bills, cheques and other instruments, or
    - foreign exchange contracts, currency, interest rate and commodity and any other derivative

- instrument in whatsoever name it is called, or
    - letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;
  - vii. collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.
  - viii.all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.
- B. Information to be preserved:  
Company shall maintain the following information in respect of transactions referred to in Rule 3 of PMLA –
- a. the nature of the transactions;
  - b. the amount of the transaction and the currency in which it was denominated;
  - c. the date on which the transaction was conducted; and
  - d. the parties to the transaction.
- C. Maintenance and preservation of records
- a. The Company shall maintain the records of all transactions including the records containing information in respect of transactions referred to in Rule 3 above in Paragraph 9.B. The Company shall take appropriate steps to 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. Further, the Company shall maintain for at least 10 (ten) years from the date of transaction between the Company and its Customers, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity; and
  - b. The Company shall ensure that records pertaining to the identification of the Customers, the designated individuals and his or her address (e.g., copies of documents like passports, identity cards, driving licenses, PAN, card, utility bills etc.) obtained while onboarding the Customers and during the course of business relationship with the Customers, are properly preserved for at least 5 (five) years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.
  - c. Company shall maintain proper records of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, including: - Cash Transaction Reports (CTR) - Suspicious Transaction Reports (STR) - Cross-border Wire Transfer Reports (CBWTR) - Non-Profit Organisation Transaction Reports (NTR) - Immovable Property Reports (IPR) e) The Company shall maintain all necessary information.
- D. Reporting to Financial Intelligence Unit – India and Obligations under International Agreements
- a. Where the Company forms a suspicion of money laundering or terrorist financing during the course of business, 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 Suspicious Transaction Report (“STR”) with FIU-IND.
  - b. The Principal Officer of the Company shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:  
Director, FIU-IND,  
Financial Intelligence Unit India,  
6th Floor, Kautilya Marg, Hotel Samrat, Chanakyapuri New Delhi 110021  
Website - <http://fiuindia.gov.in/>
  - c. Staff must not inform the customer about the filing or potential filing of an STR to ensure compliance with the tipping-off provisions under PMLA.
  - d. The Company shall scrupulously adhere to the following: (a) the Cash Transaction Report (“CTR”) for each month should be submitted to FIU-IND by 15th of the succeeding month; and (b) all cash transactions, where

- forged or counterfeit Indian currency notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions (i.e., Counterfeit Currency Report). For each month should be reported by the Principal Officer to FIU-IND by 15th of the succeeding month
- e. Suspicious Transaction Reports (“STR”): The STR shall be furnished within 7 (seven) days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. ASK Financial Holdings prepares and submits STRs when suspicious activity is identified.. Such report shall be made available to the competent authorities on request.
  - f. The Company shall ensure that it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned Lists shall be verified by the Company on a daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.
  - g. The Company shall also report the details of accounts resembling any of the individuals/entities in the sanction lists circulated by the United Nations Security Council (‘UNSC’) to FIU-IND apart from informing the Ministry of Home Affairs (MHA) as required under Unlawful Activities (Prevention) (UAPA) Act, 1967 read with UAPA notification dated February 2, 2021.
  - h. The Company shall ensure compliance with the procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of the KYC Master Direction) with regard to the freezing of assets under Section 51A of UAPA, 1967.
  - i. The Company shall verify every day, the ‘UNSCR 1718 Sanctions List of Designated Individuals and Entities’, as available at <https://www.mea.gov.in/Implementationof-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the ‘Implementation of Security Council Resolution on Democratic People’s Republic of Korea Order, 2017’, as amended from time to time by the Central Government.
  - j. 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.
  - k. The Company shall run a check, on the parameters given in Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, 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 appearing therein are holding any funds, financial asset, etc., in the form of bank account, etc.
  - l. In case the borrower details matches with the designated list circulated under 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, the Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. The Company shall file an STR with FIU-IND (CNO for the above purpose) covering all transactions in the accounts, covered above, carried through or attempted.
  - m. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the Company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
  - n. In case an order to freeze assets under Section 12A is received by the Company from the CNO, the Company shall, without delay, take necessary action to comply with the Order.
  - o. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by RE along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working

days.

- p. The Company 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.
- q. The employees of Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

#### 10. Risk Management

- A. The Management under the supervision of the Board of Directors of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures applicable to Company are implemented effectively. The Company shall devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship. The Company ensures that its due diligence machinery is staffed adequately with individuals who are well-versed in such policies and procedures.
- B. The Company shall prepare a profile for each new customer during the credit appraisal based on risk categorization as mentioned in this policy. The customer profile shall contain the information relating to the customer's identity, social/financial status, nature of business activity, information about his clients' business and their location, etc. The nature and extent of due diligence will depend on the risk perceived by Company. At the time of credit appraisal of the applicant the details are recorded along with his profile based on meeting with the applicant (by the Company representative) apart from collection of applicable documents, this will be as per the Credit/ products norms as may be in practice. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes.
- C. The Company will classify the accepted Customers into three risk categories, viz. Low, Medium and High. Risk categorization will be undertaken based on parameters such as Customer's identity, background of the Customer, social/financial status, nature of business activity, and information about the Customer's business and their location etc. The Company shall ensure that various other information collected from different categories of Customers relating to the perceived risk is non- intrusive. While considering Customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. The risk categorization of the Customers shall be in accordance with the process determined by the Company. The risk categorisation of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
- D. For the purpose of risk categorization, 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, will be categorised as low risk. These customers include salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.
- E. Customers that are likely to pose a higher than average risk to the company will 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. Company will apply enhanced due diligence measures 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. Examples of customers requiring higher due diligence include (a) non- resident customers, (b) high net worth individuals, (c) trusts, charities, NGOs and organizations receiving donations, (d) companies having close family shareholding or beneficial ownership, (e) firms with 'sleeping partners', (f) politically exposed persons (PEPs) of foreign origin, heads of states, senior politicians, and executives of state-owned enterprises. (g) non-face to face customers, and (h) those with dubious reputation as per public information available, etc.
- F. Accounts of PEPs and their close associates shall undergo Enhanced Due Diligence (EDD), including senior management approval for account opening, source of funds verification, and ongoing transaction monitoring.
- G. The Company shall adopt a risk-based approach for periodic updation of KYC. Such periodic updation of KYC shall be carried out at least once in every 2 (two) years for high-risk customers, once in every 8 (eight) years for medium

risk customers and once in every 10 (ten) years for low risk customers from the date of on-boarding of the relevant Customer or last KYC updation.

- H. The outcome of the Risk Assessment exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and shall be made available to competent authorities and self-regulating bodies.
- I. The risk assessment process will be reviewed at periodic intervals not exceeding 1 year.
- J. Group-wide KYC/AML policies and consolidated risk assessment will be implemented

#### 11. Employee Due Diligence and Training Program

- A. Adequate screening mechanism, including Employee Due Diligence shall be followed by the Company at all times in line with the Hiring Policy of the Company.
- B. The Company will ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company promotes an environment which fosters open communication and high integrity amongst the staff.
- C. Company has an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.
- D. Training requirements shall have different focuses for frontline staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.
- E. The frequency of training would be atleast annually.

#### 12. Background Search

Background searches, whether performed in-house or out-sourced, should include a comprehensive search of publicly available data using appropriate tools, such as products from commercial database search companies (e.g., Lexis-Nexis, West Law, Regulatory Data Corporation, World-Check, World Compliance, ISI Emerging Markets, Dow Jones Factiva, Owens Online), and at a minimum ensure coverage of: (i) politically exposed persons (PEPs), (ii) U.S. and, UN sanctions, as well as any other sanctions as required by applicable law, (iii) international and local adverse media, and (iv) criminal enforcement history. Different commercial database companies offer different products, and the Company will assess, from time to time, which provider to work with or establish tools and mechanisms to gather its own data, taking into consideration local realities and applicable laws.

#### 13. Confidentiality of Customers data:

- A. The Company shall treat the information collected from the Customers for the purpose of entering into business relationship with the Company as confidential and shall not divulge any details for cross selling or any other like purposes, without the prior written consent of the Customers. The Company shall ensure that information sought from the Customer is relevant to the perceived risk and is not intrusive. Any other information from the Customers shall be sought separately with their consent. No employee is permitted to share the hard copies any of the documents and/ or the information contained in them with any third party.
- B. While considering the requests for data/information from Government and other agencies, the Company 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.
- C. However, the Company shall share customer's information in the following circumstances as an exception:
  - i. Where disclosure is under compulsion of law;
  - ii. Where there is a duty to the public to disclose;
  - iii. the interest of Company requires disclosure; and
  - iv. Where the disclosure is made with the express or implied consent of the customer.

#### 14. Internal Control System:

- A. The Company's internal audit and operations functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an

- independent evaluation of the company's own policies and procedures, including legal and regulatory requirements and the said shall be implanted by the operation function
- B. Company shall ensure that its audit machinery is staffed adequately with individuals who are well versed in such policies and procedures. Concurrent/ Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard.
  - C. The adherence in this regard shall be put up before the Risk Management Committee of the Board on quarterly intervals by the risk function
  - D. Additionally, the Company will get independent evaluation of its KYC Policy and Procedures done by a third party agency at periodic intervals.
  - E. The Company shall accept Aadhaar Face Authentication as a valid mode of KYC verification for V-CIP liveness check and implement inclusive liveness checks beyond eye-blinking, accommodating customers with special needs authentication as per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025:

15. Principal Officer and Designated Director The Company shall ensure that the only a management level officers shall be appointed as a Principal Officer as per RBI (Non-Banking Financial Companies – Know Your Customer) Directions, 2025.

- A. The Board of Directors of Company has designated Mr. Dhiren Mehta, Director as the Designated Director of the Company (“Designated Director”) who shall ensure overall compliance with the obligations imposed under the PML Act and the Rules; and
- B. Ms. Ketaki Sawant, Compliance Officer, as the Principal Officer of the Company (“Principal Officer”) who shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. Principal Officer shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and combating financing of terrorism.
- C. The Company shall report name, designation, address and contact details of the Designated Director and Principal Officer to the Financial Intelligence Unit – India (“FIU-IND”) and RBI.
- D. The Company shall intimate the following details to BOTH FIU-IND and RBI:  
For Designated Director: -  
Name: Mr. Dhiren Mehta - Designation: Managing Director & Chief Executive Officer - Address: Birla Aurora, 16 Level, Office Floor 9, Dr. Annie Besant Road, Worli, Mumbai, Maharashtra - 400030 - Email: Dhiren.metha@askgroup.in
- E. For Principal Officer: - Name: Mrs. Ketaki Prasad Satam - Designation: Head – Compliance Officer - Address: [Company Address] - Email: Ketaki.sawant@askgroup.in
- F. Intimation to FIU-IND: - Through FIU-IND online portal - Within 7 days of appointment/change
- G. The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 of PML Rules to the Director, FIU-IND on the basis of information available with the Company. A copy of such information shall be retained by the Principal Officer for the purposes of official record.

#### 15. General

##### A. Customer Education

Company shall educate the Customer on the objectives of the KYC program so that customer understands and appreciates the motive and purpose of collecting such information.

##### B. Introduction of new technologies

- a. Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering. Company shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment.
- b. The Company shall identify and assess the Money Laundering (ML)/Terrorist 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 preexisting products.
- c. Further, the Company shall undertake the ML/TF risk assessments prior to the launch or use of such products,

practices, services, technologies; and (b) adopt risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

C. Applicability to Branches and Subsidiaries outside India

The above guidelines shall also be applicable to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit as and when the Company opens overseas branches. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of Reserve Bank of India.

D. Closure of Accounts / Termination of Financing / Business Relationship

Where Company is unable to apply appropriate KYC measures due to non furnishing of information and/or non-operation by the customer, Company shall terminate Financing/Business Relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken with the approval of Chairman & Managing Director or key managerial persons authorized for the purpose.

E. Foreign Account Tax Compliance Act & Common Reporting Standard:

The Company would ensure compliance with the Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standards (CRS) guidelines as stated in the RBI's Master Direction on KYC.

F. Central KYC Registry (CKYCR):

- a. The Operation function shall ensure that the Company shall mandatorily retrieve/download the KYC Identifier of all individual customers from the Central KYC Records Registry (CKYCR) prior to onboarding. KYC records shall be verified against the CKYCR database and shall be reused where no update is required.
- b. ASK shall upload/update complete KYC records of all new individual customers to the CKYCR within three (3) days from the date of commencement of an account-based relationship or update of any customer data.

16. Review of this Policy

The Policy shall be reviewed every annually.

| Type   | Approval Authority |
|--|--------------------|
| Minor amendments (including clarifications, operational process) | MD & CEO           |
| Major amendments   | Board approval     |

Annexure I

CUSTOMER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, Company shall 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, Company shall take reasonable precautions to verify the identity of the trustees and the settlors 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', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

Company shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Company shall 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.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Company shall 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. Company shall verify the identify 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 shall be taken at a senior level which shall be clearly spelt out in Customer Acceptance policy. Company shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms will also be applied to the accounts of the family members or close relatives of PEPs.

Annexure 2

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers

| Features  | Documents (Certified Copy)  |
|---|---|
| Individuals (Applicant/ Co –Applicant)<br>– Legal name and any other names used | a. Passport<br>b. PAN card (mandatory for account opening or Form No. 60)<br>c. Voter’s Identity Card issued by Election Commission of India.<br>d. Driving license<br><br>f. Proof of possession of Aadhaar number at the discretion of the borrower unless any exemption is provided by the RBI.<br>g. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of Company<br>Note: Where Aadhaar number is submitted for |

|  |  |
|--|--|
|  | authentication under Section 7 of Aadhaar Act, e-KYC authentication through UIDAI is mandatory   |
| - Correct permanent address  | <p>(i) (i) Utility bills not more than two months old: -<br/>Electricity bill - Telephone bill - Post-paid mobile phone bill - Piped gas bill - Water bill</p> <p>(ii)(ii) Property or Municipal tax receipt</p> <p>(iii) Bank Account statement (not more than three months old)</p> <p>(iv) (iv) Pension or family pension payment orders (PPOs) issued by Government Departments or PSUs (if containing address)</p> <p>(v) (v) Letter of allotment of accommodation from: - State or Central Government Departments - Statutory or regulatory bodies - Public sector undertakings - Scheduled commercial banks - Financial institutions - Listed companies</p> <p>(vi) (vi) Leave and licence agreements with above employers for official accommodation</p> <p>(vii) (vii) Proof of possession of Aadhaar number (if containing current address)</p> <p>(viii) (viii) Letter from any recognized public authority</p> <p>(ix) (ix) Rental agreement (registered)</p> <p>(x) (x) Equivalent e-documents of the above with digital signature verification</p> |
| <p>Companies (Co – Applicant)</p> <ul style="list-style-type: none"> <li>– Name of the company</li> <li>– Principal place of business</li> <li>– Mailing address of the company</li> <li>– Telephone/Fax Number</li> </ul> | <p>i) Certificate of incorporation</p> <p>(ii) Memorandum and Articles of Association</p> <p>(iii) PAN of the company (mandatory)</p> <p>(iv) Resolution of Board of Directors and power of attorney for transaction authority</p> <p>(v) Documents as specified for individuals relating to beneficial owners, managers, officers or employees holding attorney to transact</p> <p>(vi) Names of relevant persons holding senior management positions</p> <p>(vii) Address of registered office and principal place of business (if different)</p> <p>(viii) Utility bills in company name (electricity, water, telephone - not more than two months old)</p> <p>(ix) For beneficial owner identification:<br/>- Where company is listed on Indian stock exchange, or subsidiary of listed entity - beneficial owner identification not required<br/>- For other companies - identify natural persons with &gt;10% ownership or control</p> <p>(x) Equivalent e-documents of the above with digital signature verification</p>                                  |
| <p>Partnership Firms</p> <ul style="list-style-type: none"> <li>– Legal name</li> <li>– Address</li> <li>– Names of all partners and their addresses</li> <li>– Telephone numbers of the firm and</li> </ul>               | <p>(i) Registration certificate, if registered</p> <p>(ii) Partnership deed</p> <p>(iii) PAN of the partnership firm (mandatory)</p> <p>(iv) Power of Attorney granted to a partner or an employee of the firm to</p>  |

|  |  |
|--|--|
| <p>Partners</p>  | <p>transact business on its behalf<br/>           (v) Documents as specified for individuals relating to beneficial owners, managers, officers or employees holding attorney<br/>           (vi) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses<br/>           (vii) Telephone bill in the name of firm/partners<br/>           (i) Officially valid documents for partners and Power of Attorney holders as per individual requirements<br/>           (ii)(ix) Utility bills in firm/partners name (not more than two months old)</p>  |
| <p>Trusts &amp; Foundations<br/>           – Names of trustees, settlers, beneficiaries and signatories<br/>           – Names and addresses of the founder, the managers / directors &amp; the beneficiaries<br/>           – Telephone/fax numbers</p> | <p>(i) (i) Registration certificate (if registered)<br/>           (ii)(ii) Trust deed<br/>           (iii) (iii) PAN of the trust or Form No. 60 (mandatory)<br/>           (iv) (iv) Documents as specified for individuals relating to beneficial owners, managers, officers, employees holding attorney<br/>           (v) (v) Names of beneficiaries, trustees, settlor, protector (if any) and authors of the trust<br/>           (vi) (vi) Address of registered office of the trust<br/>           (vii) (vii) List of trustees and individual documents for those acting as trustees/authorized to transact<br/>           (viii) (viii) Power of Attorney for transaction authority (if applicable) (ix) Resolution of managing body (for foundations/associations) (x) Utility bills or address verification documents (not more than two months old)<br/>           (ix) (xi) For beneficial owner identification: - Author of trust, trustees, beneficiaries with 10%+ interest - Any natural person with ultimate effective control through ownership/control chain</p> |
| <p>Societies / NGOs<br/>           – Names of trustees, settlers, beneficiaries and signatories<br/>           – Names and addresses of the founder, the managers / directors &amp; the beneficiaries<br/>           - Telephone &amp; Fax number</p>    | <p>(i) Certificate of registration, if registered<br/>           (ii) Bye laws<br/>           (iii) Power of Attorney granted to transact business on its behalf (if applicable)<br/>           (iv) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers/ directors and their addresses (if applicable)<br/>           (v) Resolution of the managing body of the foundation/association<br/>           (vi) Telephone bill or personal visit or such other documents to verify existence.</p>   |

|   |  |
|---|--|
| <p>Accounts of Proprietary Concerns<br/>-Name, Address and Activity of the Proprietary Concern.</p> | <ul style="list-style-type: none"> <li>i) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop &amp; Establishment Act, sales and income tax returns, CST / VAT certificate, Certificate registration document issued by Sales Tax / Service Tax /Professional tax authorities, license issued by the Registering Authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.</li> <li>i) Any registration / licensing documents issued in the name of the proprietary concern by the Central Government or Department, IEC (Importer Exporter Code) issued to the Proprietary concern by the office of DGFT as an Identity document for opening of account.             <ul style="list-style-type: none"> <li>iii) The 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.</li> <li>iv) Utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern.</li> <li>v) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.</li> </ul> </li> </ul> |
|---|--|

|  |  |
|--|--|
| <p>POLITICALLY EXPOSED PERSONS (PEPs)</p>    | <p>(i) All standard individual/entity documents as applicable<br/> (ii) Source of funds/wealth verification documents:<br/> - Income tax returns for last 3 years<br/> - Asset ownership proof and acquisition details<br/> - Business ownership and revenue documentation<br/> - Professional/political appointment letters<br/> (iii) Enhanced background verification reports<br/> (iv) Senior management approval documentation for account opening<br/> (v) Ongoing monitoring documentation framework<br/> (vi) Family members and close associates identification</p>                       |
| <p>HIGH NET WORTH INDIVIDUALS (HNI/UHNI)</p> | <p>Additional Documentation Requirements:<br/> (i) Source of wealth verification: - Audited financial statements (for business owners) - Investment portfolio statements - Property ownership documents with valuations - Professional qualification and income certificates<br/> (ii) Enhanced background verification: - Adverse media search reports - Litigation search certificates - Business reputation verification<br/> (iii) Complex structure documentation: - Family trust structures and beneficiaries - Holding company ownership charts - Cross-border investment documentation</p> |

### Annexure III

#### An Indicative List of Suspicious Activities Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

Transactions that do not make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited unless the business activities of the customer's furnishes a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

Accounts with large volume of credits whereas the nature of business does not justify such credits.

Attempts to avoid Reporting/Record-keeping Requirements

(i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

(ii) Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.

(iii) An account where there are several cash transactions below a specified threshold level to a void filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

(i) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business relationships, officers or directors, or its locations.

(ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

(iii) A customer who has no record of past or present employment but makes frequent large transactions.

Certain NBFC Employees arousing Suspicion.

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees/willful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Placing funds in term Deposits and using them as security for more loans
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts

## Annexure IV Definitions

The following terms, wherever used in this Policy, have the meaning ascribed to them below:

“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.

“Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner. “Customer identification” means undertaking the process of CDD.

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

- a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
- b. the Managing Partner, if the RE is a partnership firm,
- c. the Proprietor, if the RE is a proprietorship concern,
- d. the Managing Trustee, if the RE is a trust,
- e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
- f. a person who holds the position of senior management or equivalent designated as a ‘Designated Director’ in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms “Managing Director” and “Whole-time Director” shall have the meaning assigned to them in the Companies Act, 2013.

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

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

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name. “Suspicious transaction” means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

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

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