Indira In Fin Lease Limited

Know Your Customer and Anti-Money Laundering Policy

*Reviewed and updated by the Board at its meeting held on March 10, 2026.

1. BACKGROUND:

The Reserve Bank of India (RBI) has issued a number of circulars and guidelines to ensure that proper Know Your Customer (KYC) norms are followed by NBFCs and that adequate checks and measures are in place to prevent money laundering. This Know Your Customer and Anti-Money Laundering Policy (Policy) have been framed by Indira In Fin Lease Limited (the "**Company**") in line with the Master Direction - Know Your Customer (KYC) Direction, 2025 issued by the RBI, as amended from time to time ("KYC Master Directions").

2. PREAMBLE:

Through the following Policy, the Company stands committed to:

a. Accepting only those clients whose identity is established by conducting due diligence appropriate to the risk profile of the customer.
b. Recording and preserving audit trail for the transactions conducted by Customers to facilitate investigation.
c. Reporting to the Financial Intelligence Unit – India (FIU-Ind), or any other agency designated by the Reserve Bank of India, Securities and Exchange Board of India or any other regulatory body, the details of transactions of all or selected clients if and when requested or at regular frequency as may be suggested by such agencies.
d. Cooperating with investigating agencies / law enforcement agencies in their efforts to trace money laundering transactions and persons involved in such transactions.

3. OBJECTIVE:

Money laundering is the process by which persons with criminal intent or persons involved in criminal activity attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, by routing the amounts through legitimate channels such as banks and financial institutions, thereby avoiding prosecution, conviction for such criminal activities.

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand its customers and their financial dealings better which in turn help them manage the Company's risks prudently.

4. APPROACH:

The approach towards KYC Standards is based on risk perception and money laundering threats that may be posed by different types of Customers. The Company shall be largely guided by the KYC standards prescribed by RBI for NBFCs.

KYC Standards & AML measures involve a customer acceptance policy and customer identification procedure that involves enhanced due diligence for higher risk accounts and includes account monitoring for suspicious activities.

5. DEFINITIONS:

These standards constitute an essential part of risk management by providing the basis for identifying and controlling risk exposures, which the Company takes to protect itself and its genuine Customers from the risks arising out of suspicious transactions/ fraudulent customers.

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

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

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

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

iv. **'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.

v. **'Digital KYC'** means that an authorised officer of the NBFC captures a live photo of the customer and officially valid document or the proof of possession of Aadhaar (where offline verification cannot be carried out), along with the latitude and longitude of the location where such live photo is being taken, as per the provisions contained in the Act.

vi. **'Digital Signature'** shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

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

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

ix. **'Know Your Client (KYC) Identifier'** means the unique number or code that the Central KYC Records Registry assigns to a customer.

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

xi. Provided that,

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

xiii. **'Person'** has the same meaning assigned in the Act and includes:

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

xiv. **'Principal Officer'** means a NBFC's nominated officer at the management level, responsible for furnishing information as per rule 8 of the Rules.

xv. **'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 have no 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.

xvi. **'Transaction'** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
(a) opening of an account;
(b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
(c) the use of a safety deposit box or any other form of safe deposit;
(d) entering into any fiduciary relationship;
(e) any payment made or received, in whole or in part, for any contractual or other legal obligation; or
(f) establishing or creating a legal person or legal arrangement.

xvii. "**Sanctioned Person**" means a person who is identified as such pursuant to any of the sanction lists published by the relevant authorities in the U.N., U.S.A, U.K., E.U. or the World Bank, as detailed below:

- **UN Sanctions** as listed on www.un.org/terrorism Such sanctions programs include, but are not limited to, Security Council Resolutions: 751 (1992), 1267 (1999), 1518 (2003), 1521 (2003), 1533 (2004), 1572 (2004), 1591 (2005), 1718 (2006), 1737 (2006), 1970 (2011), 1988 (2011) The "ISIL (Da'esh) & Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at: https://scsanctions.un.org/ohz5jen-al-qaida.html
- The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at: https://scsanctions.un.org/3ppp1en-taliban.htm
- The 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at: https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm
- 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
- Designated lists under the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)
- Lists in the First Schedule and the Fourth Schedule of Unlawful Activities (Prevention) Act, 1967

- **EU Sanctions**, which would include but are not limited to Common Positions 2001/931/CFSP and/or 2002/402/CSFP as listed on: http://eeas.europa.eu/cfsp/sanctions/consol-listen.htm
  a. Sanctions issued by: United Kingdom (as currently set forth at: https://www.gov.uk/publications/financial-sanctions-consolidated-list-of-targets)
  b. United States (as currently set forth at: (http://www.treasury.gov/resourcecenter/sanctions/SDN-List/Pages/default.aspx)
- Persons listed on the World Bank Listing of Ineligible Firms: www.worldbank.org/debarr (or any successor website or location)

(2) Unless the context otherwise requires, terms in these Directions shall bear the meanings assigned to them below:

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

(ii) **'Customer'** means a person who is engaged in a financial transaction or activity with an NBFC and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

(iii) **'Walk-in Customer'** means a person who does not have an account-based relationship with the NBFC, but undertakes transactions with the NBFC.

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

(v) **'Customer identification'** means undertaking the process of CDD.

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

(vii) **'IGA'** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

(viii) **'KYC Templates'** means templates prepared to facilitate collating and reporting KYC data to the CKYCR, for individuals and legal entities.

(ix) **'Non-face-to-face customers**' means customers who open accounts without visiting the branch / offices of the NBFC or meeting the officials of the NBFC.

(x) **'On-going Due Diligence'** means regular monitoring of transactions in accounts to ensure that transactions are consistent with the NBFC's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

(xi) **'Periodic Updation'** means the steps taken to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the RBI.

(xiv) **'Video based Customer Identification Process (V-CIP)':** an alternative method by which an authorised official of the NBFC conducts customer identification with facial recognition and customer due diligence. This process involves a seamless, secure, live, informed- consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information which the customer furnished, through independent verification and by maintaining an audit trail of the process and the NBFC shall treat such processes complying with prescribed standards and procedures on par with face-to-face CIP for the purpose of these Directions.

V-CIP Accessibility: To ensure the process is inclusive for specially-abled persons, specific facial gestures (such as blinking or smiling) are not mandatory for the liveness check if they hinder identification, provided the official can otherwise verify the customer is live and the process is secure.

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

6. NO RELATIONSHIP WITH SANCTIONED PERSONS

Neither the Company nor its subsidiaries shall do any business with any Sanctioned Person.

7. CUSTOMER ACCEPTANCE POLICY (CAP):

Before accepting a Customer, the Company shall ensure the following:

a. Any new Customer that is a financial institution shall be accepted only after it has satisfied the underwriting guidelines and eligibility criteria through a proper due diligence process and has been approved by the Credit Committee, as per internal policies. In respect of all new Customers (whether financial institutions or otherwise), the procedure prescribed under Clause 8 (Customer Identification Procedure) shall be strictly adhered to.

   No transaction or account-based relationship shall be undertaken without completing the Customer Due Diligence (CDD) process in accordance with applicable regulatory requirements.

   Any additional information, not specified in the internal KYC Policy, shall be obtained only with the explicit consent of the Customer.

b. The Company shall clearly specify and obtain mandatory KYC information and documentation at the time of onboarding and during periodic updation. The nature and extent of documentation shall be based on the risk categorisation of the Customer and shall be in accordance with the requirements of the Prevention of Money Laundering Act, 2002, rules made thereunder, and guidelines issued by the Reserve Bank of India (RBI) from time to time, as detailed in Annexure 1.

c. The Company shall undertake sanctions screening and customer verification prior to onboarding to ensure that the identity of the Customer does not match with any individual or entity appearing in:
   - Sanctions lists prescribed under RBI KYC Directions
   - Watchlists issued by regulatory authorities
   - Internal negative lists

   The Company shall also carry out automated and/or manual screening for adverse media from publicly available sources.

   Such screening shall extend, where applicable, to beneficial owners and key managerial personnel (as defined under the Companies Act, 2013), particularly in cases where the Company's exposure exceeds INR 5 crore. Relevant records shall be obtained and maintained.

d. The Company shall prepare a Customer Profile, based on risk categorisation, containing information relating to the Customer's identity, social and financial status, nature of business activity, location, and other relevant details.

   Such Customer Profile shall be treated as confidential and shall not be used for cross-selling or any purpose other than risk management and regulatory compliance.

e. A Unique Customer Identification Code (UCIC) shall be allotted to each Customer at the time of establishing a relationship. The CDD process shall be conducted at the UCIC level. Accordingly, where an existing KYC-compliant Customer seeks to open another account or avail any additional product or service, fresh CDD shall not be required for identification purposes, unless there is a material change in information.

f. No account shall be opened in an anonymous, fictitious, or benami name.

g. No account shall be opened where the Company is unable to apply appropriate CDD measures due to:
   - Non-cooperation of the Customer, or
   - Non-reliability or inadequacy of the documents/information furnished.

   In such cases, the Company shall not proceed with the relationship and shall consider filing a Suspicious Transaction Report (STR) with FIU-IND, where deemed necessary.

h. In case of joint accounts, the CDD procedure shall be conducted for all joint account holders.

i. The Company shall clearly identify and document circumstances where a Customer is permitted to act on behalf of another person or entity, and in such cases, obtain and verify:
   - Proper authorisation documents
   - Identity of the beneficial owner and the person acting on behalf
   - in accordance with applicable KYC guidelines.

j. The Company may rely on Customer Due Diligence carried out by a third party, provided that:
   - The third party is a regulated and supervised entity
   - The third party has adequate systems for compliance with KYC and record-keeping requirements under the Prevention of Money Laundering Act, 2002

   The Company shall ensure that:
   - Records or information of CDD carried out by the third party are obtained within two days or from the Central KYC Records Registry (CKYCR)
   - Copies of identification data and relevant documentation are made available by the third party without delay upon request

k. The Company shall verify, where applicable:
   - Permanent Account Number (PAN) from the issuing authority
   - Goods and Services Tax Identification Number (GSTIN) from the relevant database

- Digital signatures on electronic documents in accordance with the provisions of the Information Technology Act, 2000

l. The Customer Acceptance Policy shall ensure that it does not result in denial of financial services to members of the general public, particularly those who are financially or socially disadvantaged. Any decision to reject a Customer shall be based on proper evaluation, and the reasons for such rejection shall be recorded in writing. The Company shall ensure that no application is rejected without due application of mind.

m. Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that carrying out the CDD process may tip-off the Customer, it shall not pursue the CDD process and shall instead file a Suspicious Transaction Report (STR) with FIU-IND, in accordance with applicable regulations.

Accessibility for Persons with Disabilities (PwD) & Reasoned Rejection: The Company is committed to providing financial services without discrimination. No person shall be denied services solely on the grounds of a disability. Any decision to reject a customer whether during initial onboarding or periodic updation shall not be based solely on automated systems. A designated official must review the case and record the specific reasons for rejection in writing.

8. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

The Company shall undertake identification of Customers in the following cases:

A. Commencement of an account-based relationship with the Customer.

B. Carrying out any international money transfer operations for a person who is not an account holder of the Company.

C. When there is a doubt about the authenticity or adequacy of the Customer identification data previously obtained.

D. Selling third-party products as agents, selling its own products, payment of dues of credit cards, sale or reloading of prepaid / travel cards, or any other product for an amount exceeding INR 50,000.

E. Carrying out transactions for a non-account-based Customer (walk-in Customer), where the amount involved is equal to or exceeds INR 50,000, whether conducted as a single transaction or several transactions that appear to be connected.

F. When the Company has reason to believe that a Customer (account-based or walk-in) is intentionally structuring transactions into a series below the threshold of INR 50,000.

G. The Company shall ensure that it does not seek or rely upon introductions while opening accounts.

8.1. Identification of Individual Customers

The Company shall collect and verify Customer identification details in accordance with Annexure 2 and such other documents as may be prescribed by regulatory authorities (including RBI, UIDAI, etc.) from time to time.

Aadhaar Face Authentication: In addition to biometric and OTP-based verification, the Company may use Aadhaar Face Authentication as a valid mode of KYC identification, carried out in compliance with UIDAI and RBI standards.

The Company shall ensure that the validity and authenticity of such documents are verified through reliable and independent sources in accordance with applicable regulatory requirements.

8.2. Identification of Non-Individual Customers

In respect of Customers that are corporates or other juridical entities, the Company shall:

a. Verify the legal status of the entity through appropriate and relevant documents as specified in **Annexure 2**.

b. Verify that any person purporting to act on behalf of the entity is duly authorised, and identify and verify the identity of such person.

c. Identify and verify the Beneficial Owner(s) and obtain adequate information to establish ownership and control structure, including KYC documents of such Beneficial Owner(s), as per **Annexure 2**.

8.3. Determination of Beneficial Owner (BO)

For the purpose of this Policy:

i. Company:
The Beneficial Owner is the natural person(s), acting alone or together, or through one or more juridical persons, who:

- has a controlling ownership interest (more than 10% of shares, capital, or profits), or
- exercises control through other means

ii. Partnership Firm:

The natural person(s) who:

- has ownership of or entitlement to more than 10% of capital or profits, or
- exercises control through other means

iii. Unincorporated Association / Body of Individuals:

The natural person(s) who:

- has ownership of or entitlement to more than 15% of property, capital, or profits

iv. Where no natural person is identified:

- The Beneficial Owner shall be the senior managing official

v. Trust:

The Beneficial Owner shall include:

- Author of the trust
- Trustee(s)
- Beneficiaries with 10% or more interest
- Any other natural person exercising ultimate effective control

vi. Listed Entities:

Where the Customer or controlling owner is:

- A company listed on a recognised stock exchange, or
- A subsidiary of such company

it shall not be necessary to identify and verify individual shareholders or Beneficial Owners.

8.4. Reliance on Third-Party CDD

The Company may rely on Customer Due Diligence carried out by a third party, subject to the following conditions:

a. The Company shall obtain records or information of the CDD carried out by the third party immediately, or from the Central KYC Records Registry (CKYCR).

b. The Company shall take adequate steps to ensure that the third party makes available copies of identification data and other relevant documentation without delay upon request.

c. The third party is regulated, supervised, or monitored for compliance with KYC and record-keeping requirements under the Prevention of Money Laundering Act, 2002.

d. The third party is not based in a country or jurisdiction classified as high-risk.

e. The Company shall retain the ultimate responsibility for Customer Due Diligence (CDD) and any enhanced due diligence measures, as applicable.

8.5. Verification and Risk Management

The Company may verify Customer identity, including that of the Beneficial Owner, using reliable, independent sources of information.

The Company shall also:

- Establish procedures to identify and resolve discrepancies in Customer information
- Define escalation mechanisms and decision-making authority
- Decline or discontinue relationships where it is unable to form a reasonable belief regarding the true identity of the Customer

9. EXISTING CUSTOMER:

The requirements of the earlier sections are not applicable to transactions conducted prior to, on or after the effective date of this Policy by existing Customers, provided that the Company has previously verified the identity of the Customer and the Company continues to have a reasonable belief that it knows the true identity of the Customer. Further, the existing transactions should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

10. IDENTIFICATION OF BENEFICIAL OWNER

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to verify their identity shall be undertaken keeping in view the following:

Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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.

11. REPORTING

A. The Company shall comply with the reporting requirements prescribed under the Prevention of Money Laundering Act, 2002, the rules made thereunder, and the RBI Master Direction – Know Your Customer (KYC), as amended from time to time. The Company shall furnish to the Director, Financial Intelligence Unit–India (FIU-IND), information relating to transactions specified under Rule 3 of the PML (Maintenance of Records) Rules, 2005, including Cash Transaction Reports (CTR), Suspicious Transaction Reports (STR), and such other reports as may be prescribed, in accordance with Rule 7 and the guidelines issued by FIU-IND. The Principal Officer shall be responsible for timely and accurate electronic submission of such reports using the formats, utilities, and procedures prescribed by FIU-IND, and shall ensure proper consolidation of transaction data from all business segments, including those not fully automated.

B. The Company shall establish an effective system of internal monitoring and reporting of transactions, including single transactions, integrally connected transactions, and attempted transactions, to identify and report suspicious activities. Where the Company has reason to believe that any transaction or series of transactions is suspicious or is structured to avoid regulatory thresholds, including the prescribed cash limits, the Principal Officer shall file an STR with FIU-IND within the prescribed timelines, irrespective of whether the transaction is completed or attempted. The Company shall ensure that delays in reporting or rectification of misreported transactions are avoided, as each day of delay beyond the prescribed timelines shall constitute a separate violation. The Company shall not restrict or discontinue operations in any account solely on the basis of filing an STR.

C. The Company, its Directors, officers, and employees shall maintain strict confidentiality in respect of records maintained and information furnished to FIU-IND and shall ensure that there is no tipping-off to the Customer or any third party regarding the filing of STRs or related processes. The Company shall implement robust systems, including technology-based solutions, for transaction monitoring and alert generation to identify transactions inconsistent with the Customer's risk profile.

D. In case of identification of accounts or transactions matching with individuals or entities listed under the United Nations Security Council (UNSC) Sanctions Lists, or those notified under the Unlawful Activities (Prevention) Act, 1967 or the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, the same shall be immediately escalated to the Principal Officer, who shall report such cases to FIU-IND, the

Ministry of Home Affairs, the Central Nodal Officer, and other authorities as required, and file an STR covering such transactions. The Company shall also ensure strict compliance with directions relating to freezing of assets under Section 51A of the UAPA and applicable Government notifications. Any request for unfreezing of assets under the WMD Act shall be forwarded by the Principal Officer to the Central Nodal Officer, FIU-India, within the prescribed timelines along with complete details.

E. The Company does not accept deposits and generally does not permit cash transactions, except limited collections in the MFI segment and authorised recovery cases, which shall be within applicable legal limits and subject to enhanced monitoring and reporting requirements.

12. RECORD MANAGEMENT / RECORD RETENTION

The Company shall maintain, preserve, and report customer and transaction records in accordance with the provisions of the **Prevention of Money Laundering Act, 2002**, the rules made thereunder, and the **RBI Master Direction – Know Your Customer (KYC)**, as amended from time to time. The Company shall ensure that all records are accurate, complete, readily retrievable, and available to competent authorities as and when required.

The Company shall adhere to the following principles:

- **Maintenance of Transaction Records:** All records of transactions, whether domestic or international, shall be maintained for a minimum period of **five (5) years from the date of transaction**.

- **Preservation of KYC Records:** Records relating to customer identification, including account files, business correspondence, and results of any analysis undertaken, shall be preserved for at least five (5) years after the business relationship has ended or the account has been closed, whichever is later.

- **Coverage of Reportable Transactions:** The Company shall maintain records of transactions as prescribed under Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, including:
  i. Cash transactions and integrally connected transactions
  ii. Transactions involving counterfeit currency or forgery
  iii. Suspicious transactions, whether attempted or executed

- **Minimum Information Requirements:** Records maintained shall be sufficient to permit reconstruction of individual transactions, including:
  i. Nature of transaction
  ii. Amount and currency

iii. Date of transaction
iv. Parties to the transaction

- **Record Maintenance System:** The Company shall implement appropriate systems (including electronic systems) to ensure proper maintenance, secure storage, and easy and quick retrieval of records.

- **Availability to Authorities:** All records shall be made available **swiftly to competent authorities** upon request, in accordance with applicable laws and regulatory requirements.

- **Mode of Storage:** Records may be maintained in physical or electronic form, subject to ensuring integrity, confidentiality, and accessibility.

- **Non-Profit Organisation (NPO) Compliance:** In case of customers classified as non-profit organisations, the Company shall ensure that such entities are registered on the DARPAN Portal of NITI Aayog, where applicable, and shall maintain such registration records for a period of five (5) years after the end of the business relationship or closure of account, whichever is later.

13. ENHANCED DUE DILIGENCE

The Company shall undertake Enhanced Due Diligence (EDD) measures in accordance with the RBI Master Direction – Know Your Customer (KYC), as amended from time to time, particularly in cases of non-face-to-face customer onboarding and other high-risk relationships.

Customers onboarded without meeting physically or through the Video-based Customer Identification Process (V-CIP) shall be classified as high-risk customers and shall be subjected to enhanced monitoring until their identity is verified through face-to-face interaction or V-CIP.

In respect of non-face-to-face onboarding, the Company shall implement the following EDD measures:

- Where the Company has implemented V-CIP, it shall be provided as the first option for remote onboarding, and processes complying with prescribed standards shall be treated at par with face-to-face Customer Identification Procedure.
- To prevent fraud, alternate mobile numbers shall not be linked post CDD for transaction OTPs, alerts, or updates. Transactions shall be permitted only through the mobile number registered at the time of onboarding. Any request for change in mobile number or other key details shall be processed only after appropriate due diligence, as per the Company's Board-approved policy.
- In addition to obtaining proof of current address, the Company shall carry out positive confirmation of the address (such as through verification letters, contact point verification, or equivalent methods) before permitting operations in the account.
- The Company shall obtain and verify the Permanent Account Number (PAN) of the Customer through the verification facility of the issuing authority.

- The first transaction in such accounts shall be a credit from an existing KYC-compliant bank account of the Customer.

The Company shall adopt a Risk-Based Approach (RBA) for identification, assessment, and mitigation of money laundering and terrorist financing risks. The Company shall conduct a periodic Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment, at least on an annual basis, taking into account factors such as customer profile, geographic risk, products, services, transactions, and delivery channels. The outcome of such assessment shall be placed before the Audit Committee of the Board.

Customers identified as high-risk shall be subjected to enhanced due diligence and ongoing monitoring, commensurate with the level of risk. The Company may, where necessary, make use of independent sources, external databases, or investigative services for additional verification.
The Company shall establish procedures to decline onboarding or discontinue business relationships where it is unable to satisfactorily complete enhanced due diligence or where the information obtained gives rise to significant reputational or regulatory concerns.

Further, the Company shall put in place a system for periodic review of customer risk categorisation, with such review being carried out at least once every six months, and shall determine the continued applicability of enhanced due diligence measures.

14. MONITORING OF TRANSACTIONS

Monitoring of Transactions and Ongoing Due Diligence
The Company shall undertake **ongoing due diligence** of Customers to ensure that transactions are consistent with its knowledge of the Customer, the Customer's business, risk profile, and source of funds/wealth. The extent of monitoring shall be **risk-based**, with higher scrutiny applied to high-risk Customers.

The Company shall pay special attention to transactions including:
- Large and complex transactions, including high-value transfers
- Transactions with unusual patterns or inconsistent with the Customer's profile
- Transactions lacking apparent economic or lawful purpose
- High account turnover inconsistent with the Customer profile
- Structured transactions or those exceeding prescribed thresholds

The Company may deploy automated monitoring systems and analytics tools to effectively identify and report suspicious transactions.

The Company shall carry out a periodic review of risk categorisation of Customers at least once every six months, and determine the need for applying enhanced due diligence measures. As an

additional control, the Company may also monitor the end-use of funds, wherever contractually agreed.

14.1. Risk-Based Categorisation: Customers shall be categorised into High, Medium, and Low Risk based on parameters such as identity, business activity, geography, product usage, and transaction behaviour. Such categorisation shall be kept confidential and reviewed periodically.

- **High Risk:** Includes non-residents, PEPs, non-face-to-face Customers, entities with complex ownership, adverse media cases, high-risk industries, and Customers linked to suspicious transactions or frauds.

- **Medium Risk:** Includes Customers with moderate risk profiles such as private companies, LLPs, partnerships, and others not falling under high or low risk.

- **Low Risk:** Includes salaried individuals, small borrowers, regulated entities, government bodies, and Customers with stable and transparent profiles.

- **Transition Relief for Low-Risk Customers**: Notwithstanding the standard periodicities, for all low-risk customers whose KYC updation fell due, the timeline for completion is extended to June 30, 2026, or one year after the original due date, whichever is later

14.2. Periodic Updation of KYC: The Company shall carry out periodic updation of KYC as per the following minimum periodicity:

- **High Risk:** Every 2 years
- **Medium Risk:** Every 8 years
- **Low Risk:** Every 10 years

For low-risk individual Customers, continued operations shall be allowed as per regulatory relaxations, while ensuring timely updation and regular monitoring.

Updation Process:

Facilitation via Business Correspondents (BCs): Authorized BCs and field agents are empowered to facilitate the periodic KYC updation process by collecting self-declarations and required documents electronically through the Company's authorized digital applications

- **No change in KYC:** Self-declaration through registered channels
- **Change in address:** Self-declaration + positive confirmation within 2 months
- **Minor attaining majority:** Fresh KYC / updated documents to be obtained
- **Non-individuals:**
    i. No change → self-declaration + BO confirmation
    ii. Change → fresh KYC equivalent to onboarding

Additional Controls

- Ensure KYC documents are as per current CDD standards
- Verify PAN from issuing authority during updation
- Provide acknowledgement and update records promptly
- Enable KYC updation through digital/branch channels
- Customers shall update KYC documents within 30 days of any change

14.3. Temporary Cessation of Operations: In case of failure to submit **PAN / Form 60** within prescribed timelines:

- The Company may **temporarily cease operations** after prior notice and opportunity to be heard
- In loan accounts, only **credits shall be permitted**
- Relaxation may be granted in genuine cases, subject to **enhanced monitoring**

14.4 Customer Communication

The Company shall:

- Provide **advance intimations and reminders** for KYC updation
- Include clear instructions and escalation mechanism
- Maintain **audit trail** of all communications

15. ADHERENCE

The Company's operations function shall ensure adherence to the KYC policies and procedures. The Company's internal audit and compliance functions have an important role in auditing adherence to the KYC policies and procedures. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals.

The Company shall have an ongoing employee training programme so that the employees conducting the KYC are adequately trained in KYC procedures. It is crucial that all concerned employees fully understand the rationale behind the KYC policies and implement them consistently.

The senior management for the purpose of KYC Compliance shall include Chief Executive Officer, Chief Financial Officer, Group Risk Officer and Governance Head, Chief Internal Auditor, Chief Compliance Officer, Chief Risk Officer, Head - Operations and Chief Legal Counsel.

Customer Education

If required, the Company may prepare specific literature / pamphlets etc. to educate the Customer of the objectives of the KYC programme.

16. APPLICABILITY TO BRANCHES AND SUBSIDIARIES OUTSIDE INDIA

Presently, the Company does not have any branches and subsidiaries outside India. However, if the Company establishes such a branch or a majority owned subsidiary, which is located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, the Company shall ensure that the above guidelines are also implemented in these locations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of Reserve Bank of India.

Principal Officer and Designated Director

Mr. Akshay Kamdar (DIN: 03024269) Director of the Company shall be designated as Principal Officer for the purpose of compliance with the rules and regulations of this policy. The Principal Officer can be contacted at the following address:

Attn: Mr. Atul Kamdar (DIN: 00609527) Director of the Company
Address: 4402, 44th Floor, B Wing, Three Sixty West,
Annie Besant Roda, Worli, Mumbai 400025.

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

Mr. Akshay Kamdar (DIN: 03024269) Director shall be nominated as Designated Director to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

17. SECRECY OBLIGATIONS AND SHARING OF INFORMATION

17.1 Secrecy Obligations

The Company shall maintain strict confidentiality of Customer information obtained in the course of its business relationship and shall ensure that such information is not disclosed to any third party, except as permitted under applicable laws and regulations.

While considering requests for information from Government authorities or other agencies, the Company shall ensure that such disclosure is in compliance with applicable legal and regulatory requirements and does not violate the provisions relating to secrecy of customer information.

Disclosure of customer information shall be permitted only under the following circumstances:

- Where disclosure is required under compulsion of law
- Where there is a duty to the public to disclose

- Where the interest of the Company requires disclosure
- Where disclosure is made with the express or implied consent of the Customer

The Company shall ensure compliance with the provisions of Section 45NB of the RBI Act, 1934 and other applicable laws relating to confidentiality and data protection.

Further, the Company shall ensure that no information relating to suspicious transactions or STR filings is disclosed to the Customer or any unauthorised person, in order to prevent tipping-off.

17.2 Sharing of Information with Authorities and Regulators

The Company shall furnish information to regulatory and enforcement authorities, including FIU-IND, RBI, and other competent authorities, as required under applicable laws, including the Prevention of Money Laundering Act, 2002, and rules made thereunder.

Where applicable, the Company may also share information with other regulated entities or group entities, strictly on a need-to-know basis, and in compliance with regulatory requirements.

17.3 Sharing of Information with Central KYC Registry (CKYCR)

The Company shall capture, maintain, and upload Customer KYC records with the Central KYC Registry (CKYCR), in accordance with the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, and guidelines issued thereunder.

- KYC data shall be uploaded in the prescribed format and timelines
- The Company shall use the KYC Identifier for retrieval and updation of records
- Any changes in Customer information shall be updated in CKYCR promptly

17.4 Policy Review

This Policy shall be reviewed periodically by the Management to ensure continued alignment with applicable laws and regulatory requirements. A consolidated review report shall be placed before the Board of Directors at least annually, or earlier in case of significant regulatory changes.

17.5 Independent Assessment:

An independent assessment of the implementation and effectiveness of this Policy shall be conducted at least annually by internal auditors or other independent functions. The observations and recommendations arising from such review, including compliance with RBI Master Directions and statutory requirements, shall be placed before the Audit Committee of the Board for appropriate action.

Annexure 1

Customer Identification Requirements

TRANSACTIONS WITH TRUST / NOMINEE OR FIDUCIARIES

There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the Customer Identification Procedure.

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

While conducting a transaction with a trust, the 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.

TRANSACTIONS WITH COMPANIES AND FIRMS

The Company shall be vigilant against business entities being used by individuals as a 'front' for conducting transactions with the Company.

The 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.

TRANSACTIONS WITH POLITICALLY EXPOSED PERSONS (PEPS) RESIDENT OUTSIDE INDIA

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

The 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.

The Company shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a Customer.

The Company shall also subject such transactions enhanced monitoring on an ongoing basis. The above norms may also be applied to transactions with the family members or close relatives of PEPs.

The decision to accept a PEP as a Customer shall be taken by the Credit Committee, or the relevant credit decision-making authority.

ANNEXURE 2
LIST OF ACCEPTABLE KYC DOCUMENTS

Constitution	Documentary Requirements
Company	• Certificate of incorporation • Memorandum of Association or the equivalent e-document thereof • Articles of Association or the equivalent e-document thereof • PAN card of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of applicant • Equity share capital table • Share capital table on an as if converted/ fully diluted basis • Details of existing credit facilities and charges • Audited financial statements of the applicant for the last three years • Resolution passed by the Board of Directors of the applicant and power of attorney granted by the applicant to its managers, officers, employees or such other persons, as the case may be, to transact on its behalf ("Authorized Persons") • PAN card of Authorized Persons shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Certified copy of officially valid documents as proof of identity and address of Authorized Persons or the equivalent e-document thereof • Recent photograph of Authorized Persons holding an attorney to transact on behalf of the applicant • PAN card of beneficial owners of the applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Recent photograph of beneficial owners of applicant • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of beneficial owners of applicant • the names of the relevant persons holding senior management position the registered office and the principal place of its business, if it is different. • Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority

Partnership Firms and Limited Liability Partnership	• Registration certificate • Partnership deed • PAN card of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of applicant • Details of existing credit facilities and charges. • Books of accounts of the applicant for the last three years
	• Resolution passed by the managing body of the applicant and power of attorney granted by the applicant to its managers, officers, employees or such other persons, as the case may be, to transact on its behalf ("Authorized Persons") • PAN card of Authorized Persons shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of Authorized Persons • Recent photograph of Authorized Persons holding an attorney to transact on behalf of the applicant • PAN card of beneficial owners of the applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Recent photograph of beneficial owners of applicant • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of beneficial owners of the applicant • the names of all the partners • address of the registered office, and the principal place of its business, if it is different • Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority
Trust	• Registration certificate • Trust deed • PAN card of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of applicant • Details of existing credit facilities and charges. • Books of accounts of the applicant for the last three years • Resolution passed by the managing body of the applicant and power of attorney granted by the applicant to its managers,

	officers, employees or such other persons, as the case may be, to transact on its behalf ("Authorized Persons") • PAN card of Authorized Persons shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of Authorized Persons • Recent photograph of Authorized Persons holding an attorney to transact on behalf of the Applicant • PAN card of beneficial owners of the applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Recent photograph of beneficial owners of applicant
	• Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of beneficial owners of the applicant. • the names of the beneficiaries, trustees, settlor and authors of the trust • the address of the registered office of the trust • Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
Society	• Registration certificate • Memorandum of Association and bye-laws • PAN card of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of applicant • Details of existing credit facilities and charges. • Books of accounts of the applicant for the last three years • Resolution passed by the managing body of the Applicant and power of attorney granted by the applicant to its managers, officers, employees or such other persons, as the case may be, to transact on its behalf ("Authorized Persons") • PAN card of Authorized Persons shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of Authorized Persons • Recent photograph of Authorized Persons holding an attorney to transact on behalf of the applicant

	• PAN card of beneficial owners of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Recent photograph of beneficial owners of applicant • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of beneficial owners of the applicant
Unincorporated Associations or Body of Individuals	• Agreement of Association of Persons or Body of Individuals • PAN card of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of applicant • Details of existing credit facilities and charges • Books of accounts of the applicant for the last three years • Resolution passed by the managing body of the applicant and power of attorney granted by the applicant to its managers, officers, employees or such other persons, as the case may be, to transact on its behalf ("Authorized Persons") • PAN card of Authorized Persons shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of Authorized Persons • Recent photograph of Authorized Persons holding an attorney to transact on behalf of the applicant • PAN card of beneficial owners of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Recent photograph of beneficial owners of applicant • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of beneficial owners of the applicant
Proprietorship	• Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 of the proprietor. The PAN of proprietor shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Proof of address of proprietary firm • Details of existing credit facilities and charges • Books of accounts of the applicant for the last three years • Certified copy of officially valid documents or the equivalent e-document thereof as proof of identity and address of proprietor • Recent photograph of proprietor

	• Any two of the following documents or the equivalent e-document thereof as proof of business in the name of proprietary firm; (a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government, (b) certificate/license issued by municipal authorities under Shops and Establishments Acts, (c) sales and income tax returns, (d) GST certificate, (e) certificate/ registration document issued by sales tax/service tax/professional tax authorities, (f) IEC code or license/certificate of practice issued by any professional body incorporated under a statute, (g) complete income tax return (not just acknowledgment) in the name of proprietor reflecting firm's income, duly authenticated/acknowledged by income tax department, (h) utility bills such as electricity, water, landline telephone bills, etc. • Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
Individuals	• one recent photograph of the applicant • Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962. Where the collected PAN of applicant shall be verified from the search/verification facility of the issuing authority or the equivalent e-document thereof • Certified copy of officially valid documents or the equivalent e-document thereof as • proof of identity and address of the applicant. **Note on Aadhaar:** The submission of the 'Proof of possession of Aadhaar number' is voluntary for the customer unless they are seeking benefits or subsidies under Section 7 of the Aadhaar Act

Notes: The term 'officially valid documents' shall mean passport, the driving license, 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.

In case an '**officially valid document**' does not contain the updated address, the following documents shall be collected which are deemed to be officially valid documents for the limited purpose of proof of address: (a) utility bill not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) property or municipal tax receipt; (c) pension or family pension payment orders issued to retired employees by government departments or public sector undertakings, if they contain the address; (d) 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 license agreements with such employers allotting official accommodation. Provided that the applicant shall submit an 'officially valid document' containing the current address within three months of submitting the aforementioned documents.

'**Certified copy of officially valid document**' shall have the meaning assigned to it under the 'Master Direction – Know Your Customer (KYC) Direction, 2016', as issued by RBI. Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company as per the provisions contained in the Act. For the purpose of this definition, employees of the Company shall be considered as authorized officials.

"**Proof of possession of Aadhaar number**" shall be submitted in such form as permitted under the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act (including the rules, regulations and notifications issued thereunder) and in compliance with 'Master Direction – Know Your Customer (KYC) Direction, 2016' issued by RBI.

"**Beneficial Owners**" shall mean such persons identified by the applicant in the application form in terms of Rule 9
(3) of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

"Equivalent e-document" shall have the meaning assigned to it under the 'Master Direction – Know Your Customer (KYC) Direction, 2016' as issued by RBI – i.e., an electronic equivalent of a document issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000. Further, where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal.

The Company shall ensure that the customers' KYC Identifier shall be the first reference point for the purpose of establishing an account-based relationship or for verification of identity of customers. Accordingly, while onboarding customer, the Company shall download customers' KYC records online from CKYCR with customer's consent without requiring him/

her to submit the same records again, unless there is a change in records available with CKYCR.

ANNEXURE 3

Mode and Timeline for sharing Advance Intimations and Subsequent reminders for Periodic Updation

Advance Intimation			
SN	Particular	Mode	Timeline
1	Advance Intimation 1	At least one intimation by letter	Before 60 days of due date
2	Advance Intimation 2	At least one intimation by letter	Before 30 days of due date
3	Advance Intimation 3	At least one intimation by letter	Before 15 days of due date
Reminder for Periodic Updation			
SN	Particular	Mode	Timeline
1	Reminder 1	At least one intimation by letter	After 7 days of due date
2	Reminder 2	At least one intimation by letter	After 15 days of due date
3	Reminder 3	At least one intimation by letter	After 30 days of due date

(Due date shall mean the date on which periodic updation requirement become due on account of the risk categorization of the customer)