KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING POLICY

Document name	KNOW YOUR CUSTOMER AND ANTI-MONEY LAUNDERING POLICY
Version	V1.0
Document author	Compliance and secretarial Team
Release date	26th May 2025
Last updated on	26th May 2025
Review frequency	Annual
Approved by	Board of Directors

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

TABLE OF CONTENTS

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

1. INTRODUCTION

Tenmark Capital Private Limited ("**Company**", "**Tenmark**", "**we**", "**us**" or "**our**") is a Non-Deposit taking Non-Banking Financial Company ("**NBFC-ND**") registered with the Reserve Bank of India ("**RBI**"). The RBI has issued Master Direction- Know Your Customer (KYC) Direction, 2016 ("**KYC Master Directions**") including comprehensive guidelines on Know Your Customer ("**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 is formulated and put in place. The Company is committed to complying with all applicable AML laws in the conduct of its business. Our employees and its agents/representatives acknowledge that failing to detect customer relationships and transactions that place us at risk, could cause irreparable harm to our reputation, leading to significant financial loss and severe penalties under applicable law. Hence, the Board of Directors of the Company ("**Board**") has approved and adopted this KYC policy ("**Policy**") in accordance with the KYC Master Directions as amended from time to time.

2. OBJECTIVE AND SCOPE OF THE POLICY

This Policy intends to know and understand the Company's customers and their financial dealings which in turn will help the Company to manage risks and prevent the use of the Company or its infrastructure in illegal or money laundering activities. This Policy constitutes a minimum standard. In case applicable laws are stricter than this Policy, the applicable laws will prevail.

This Policy applies to our Company, its affiliates, agents/representatives and all individuals working at all levels and grades, including Senior Management, directors, senior managers, officers, other employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, interns, seconded staff, casual workers and agency staff, agents, or any other person associated with our Company.

3. DEFINITIONS

Unless the context otherwise requires, the terms used in the Policy shall bear the meanings assigned to them below and the terms not defined in the Policy shall have the same meaning as assigned to them in the KYC Master Directions:

i. "**Act**" means the Prevention of Money Laundering Act, 2002 and amendments thereto.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

ii. "**Board**" means the Board of Directors of the Company.

iii. **"Customer"** means a person, who is engaged in a financial transaction or activity with Tenmark and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iv. "**Customer Due Diligence"** or **"CDD"** means the process of identifying and verifying the customer.

v. "**Designated Director**" means a person nominated and designated by the Board to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules.

vi. "**Digital KYC**" means the process described in Annex 1 – Digital KYC Process.

vii. "**Face-to-Face Customer**" shall mean any customer who has been onboarded through a physical meeting by a person designated by TCPL.

viii. "**Non-face-to-face Customer**" shall mean any customer who is not a Face-to-Face Customer.

ix. "**Principal Officer**" shall be a person appointed by the Company who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

x. "**Rules**" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and amendments thereto.

xi. "**Senior Management**" means personnel of the company who are members of its core management team excluding Board of Directors comprising all members of management one level below the executive directors, including the functional heads.

xii. **"Cash Transactions"** means "Cash Transactions" as defined under rule 3 of the Rules.

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

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

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

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

xvi. **"KYC Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

xvii. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

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

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

xx. **"Suspicious Transaction"** means 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

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

transactions 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.

xxi. **"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.

a. Provided that 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;

4. COMPLIANCE WITH THE POLICY

i. The Senior Management shall be responsible for ensuring implementation of this Policy.

ii. The Board shall designate (a) a 'Designated Director' who shall be responsible for ensuring overall compliance with the obligations imposed under the Act and the Rules and (b) a 'Principal Officer' who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the Policy and applicable laws. In no case, the Principal Officer shall be nominated as the Designated Director.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

iii. The Company shall carry out an audit of its KYC functions and process either internally or through an external auditor on an annual basis and the report of such audit shall be placed before the Board for its review.

iv. The company shall prepare and place KYC Compliance matters to the Board on a quarterly basis.

5. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

i. The Company shall carry out a 'Money Laundering and Terrorist Financing Risk Assessment' ("**ML and TF Risk Assessment**") exercise annually to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

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

iii. Before launching any new products or business practices, the Company shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

iv. The Senior Management shall ensure that such risk assessment is properly documented and is proportionate to the nature, size, geographical presence, and complexity of the activities of the Company.

v. The outcome of the ML and TF Risk Assessment exercise shall be put up to the Board. The Board shall review the outcome and evaluate corrective measures, where required, including changes in the CDD process.

vi. The compliance officer of the Company shall ensure that the ML and TF Risk Assessment along with its outcome is adequately documented and is made available to the RBI or the self-regulatory bodies where the Company is a member.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

vii. The Company shall apply a risk-based approach for the mitigation and management of the risks identified. Further, the Board shall monitor the implementation of the controls and enhance them, if necessary.

6. CUSTOMER ACCEPTANCE POLICY

i. The Company shall not open any account in anonymous or fictitious/benami names.

ii. The Company shall not open any account unless it undertakes appropriate CDD measures. Additionally, in case the Company is unable to carry out CDD in relation to a customer, the

Company shall review the reasons for not being able to carry out the CDD and if the circumstances so require, consider filing a ("**STR**") suspicious transaction report as specified in clause 14 of this Policy.

iii. The Company shall require the customer to mandatorily submit the Permanent Account Number ("**PAN**") and any one of the officially valid documents ("**OVDs**"). It must be ensured that any optional or additional information is obtained only with the explicit consent of the customer.

iv. The Company shall apply the CDD process at the Unique Customer Identification Code ("**UCIC**") level. Thus, if an existing KYC-compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise. However, the Company may carry out a periodic updation of the customer as per the requirements under clause 15 of this Policy.

v. The PAN obtained by the Company from the customer shall be verified through the verification facility of the issuing authority.

vi. Where an equivalent e-document is obtained from the customer, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000

vii. The Company shall ensure that the identity of the customer (including their name, photograph, or other details) does not match with any person with known criminal background or with a banned entity such as individual terrorists or terrorist organisations etc. and whose name appears in the sanction lists circulated/prescribed by RBI from time to time.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

viii. Circumstances such as 1. death of a borrower 2. Permanent disability as a result of which the account holder isn't able to come. 3. Any other cases as decided by the management, upon submitting necessary proofs and documents that the management may prescribe from time to time, in which case a nominee is permitted to act on behalf of the customer, is clearly spelt out.

ix. The Company shall take adequate care to ensure that the CDD process does not result in denial of financial facilities to members of the public, especially those, who are financially or socially disadvantaged.

7. RISK MANAGEMENT

i. The Company shall follow a risk-based approach to CDD. The customers shall be categorized into the following risk categories:
   a. Low risk;
   b. Medium risk; and
   c. High risk;

ii. The risk categorization of the customers may be undertaken on the following parameters:
   a. customer's identity
   b. credit score;
   c. source of income;
   d. annual and monthly income;
   e. geographical risk;
   f. type of loan availed; and
   g. delivery channel used for extending the loan product

iii. The customer risk categorization will be done at the time of opening the loan account and monitored on a regular basis with a built-in mechanism for tracking irregular behaviour for risk management and suitable timely corrective action. It must be ensured that the risk categorisation of a customer and the specific reasons for such categorisation are kept confidential and not revealed to the customer.

iv. **High and Medium Risk from AML perspective-** A customer who is likely to pose a higher-than-average risk may be categorized as high or medium risk depending on background, nature & location of customer, his/ her profile, scale of customer's volume, his/ her financials and social status etc. Due diligence measures will be applied based on the risk

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

assessment. The Company shall apply enhanced due diligence measures for any customer whose behaviour shall indicate high risk customer's behaviour.

v. **Indicative list of High-Risk Customers**

a. Individuals and entities in watch lists issued by Interpol and other similar international organizations;
b. Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
c. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
d. Customers that may appear to be multi-level marketing companies etc.

vi. **Low Risk from AML perspective**- All other customers (other than High and Medium Risk category) whose identities and sources of wealth/income can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only

the basic requirements of verifying the identity and location of the customer are to be met.

8. CUSTOMER IDENTIFICATION PROCEDURE

The Company shall obtain sufficient information necessary to establish the identity of each customer. The Company shall undertake the identification of customers in the following cases:

i. commencement of an account-based relationship with the customer; and
ii. when there is doubt about the authenticity or adequacy of the customer identification data.

The Company shall onboard Face-to-Face Customer(s) only.

9. CUSTOMER DUE DILIGENCE BY THIRD PARTIES

The Company may rely on CDD done by a third party, subject to the following conditions:

i. records or the information of the CDD carried out by the third party are obtained immediately from the third party or the Central KYC Registry ("**CKYCR**");
ii. adequate steps are taken by the Company to ensure that copies of identification data and other relevant documentation relating to the CDD requirements are made available from the third party upon request without delay;
iii. 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 Act;

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

iv. the third party shall not be based in a country or jurisdiction assessed as high-risk;
v. the ultimate responsibility for CDD and undertaking enhanced due diligence measures, as applicable, shall remain with the Company; and
vi. the right to make decisions with respect to compliance with KYC Master Directions and this Policy rests with the Company.

10. CUSTOMER DUE DILIGENCE

i. The Company shall obtain the following documents from the customer:

a. PAN or equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962;
b. any of the OVDs or equivalent e-document thereof containing details of proof of their identity and address; and
c. such other documents as required by the Company.

ii. The Company may carry out CDD through any of the following modes:

a. offline verification;
b. verification through non-face-to-face modes such as OTP-based e-KYC, KYC through CKYCR, DigiLocker, obtaining equivalent e-document, etc.
c. Digital KYC as described in **ANNEX 1**

iii. The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the company and shall be available for supervisory review.

11. ENHANCED DUE DILIGENCE

Enhanced Due Diligence ("**EDD**") shall be carried out in case the customer is a politically exposed person ("**PEP**"). The Company may establish an account-based relationship with such customer provided the following is complied with:

i. sufficient information including information about the sources of funds, accounts of family members and close relatives, etc. is gathered;
ii. the identity of the customer is verified before establishing an account-based relationship;

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

iii. the decision to open an account for a PEP is taken by the board of directors in accordance with the Policy;
iv. all such accounts are subjected to enhanced monitoring on an ongoing basis; and
v. In the event of an existing customer becoming a PEP, the Senior Management's approval is obtained to continue the business relationship.

12. ON-GOING DUE DILIGENCE

The Company shall undertake ongoing due diligence of customers to ensure that their transactions are consistent with the Company's knowledge about the customers, customers' income profile and risk profile, and the source of funds. The extent of monitoring shall be aligned as per the risk category of the customer. Ongoing due diligence shall be undertaken for the following categories of transactions:

i. large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which has no apparent economic rationale or legitimate purpose;
ii. transactions that exceed the thresholds prescribed for specific categories of accounts; and

iii. deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
iv. remittances from outside India.

13. SECRECY OBLIGATIONS

i. The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and the customer. Information collected from customers for opening of account shall be treated as confidential and details thereof shall not be divulged for any purpose without the express permission of the customer.

ii. The exceptions to the said rule shall be as under:
   a. where disclosure is under compulsion of law;
   b. where there is a duty to the public to disclose;
   c. the interest of the Company requires disclosure; and
   d. where the disclosure is made with the consent of the customer.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

iii. While considering the requests for data/information from the government and/or other agencies, the Company shall satisfy itself that the information being sought is not of such a nature that will violate the provisions of the laws relating to the secrecy of the transactions.

14. REPORTING REQUIREMENTS

i. **Reporting to Financial Intelligence Unit-India ("FIU-IND"):** The following information is required to be submitted to the FIU-IND:

a. the name, designation and address of the Designated Director and the Principal Officer of the Company as per the timelines specified on the FIU-IND's filing portal.

b. the Principal Officer shall immediately file an STR:

- in case the Company finds a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip off the customer; and
- any other transaction, which by its nature, gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the Act, regardless of the value involved, appears to be made in circumstances of unusual or unjustified complexity, appears to have no economic rationale or bona fide purpose, or gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism or other forms of criminal activity.

c. A cash transactions report ("**CTR**") shall be submitted by 15th day of the succeeding month for all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency, which if taken together, amount to more than rupees ten lakhs, where such series of transactions have taken place within a month.

d. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed. An indicative list of suspicious transactions as given as **Annex 2**.

ii. **Reporting to CKYCR:** The Company shall capture the customer's KYC records and upload the same on the CKYCR portal within 10 days of commencement of an account-based relationship with the customer. In case of a first-time customer, a 'KYC identifier' shall be

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

generated upon submission of the KYC records to CKYCR. Once such a KYC identifier is generated by CKYCR, the Company shall communicate the same to the customer.

iii. **Reporting to the RBI:** The Company shall share the details of the Designated Director and the Principal Officer of the Company including their name, designation and address with the RBI within 30 days of the appointment of such Designated Director or Principal Officer.

iv. **Freezing of Assets under section 51A of UAPA, 1967:** The procedure laid down in the UAPA Order dated February 2, 2021, shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA

15. RESPONSIBILITIES OF THE SENIOR MANAGEMENT

a) Designated Director

- A "Designated Director" means a person designated by the Company to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.
    - The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
    - Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
    - In no case, the Principal Officer shall be nominated as the 'Designated Director'.

b) Principal Officer

- The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
- The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

c) Key Responsibilities of the senior management

- Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under PMLA.
- Proper implementation of the company's KYC & AML policy and procedures.

16. PERIODIC UPDATION

The Company shall follow a risk-based approach to periodic updation. Periodic updation shall be carried out at least once every two years for high-risk customers, once every eight years for medium-risk customers and once every ten years for low-risk customers subject to the following conditions:

i. fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorised as 'low risk', when there is no change in status with respect to their identity information and addresses. In such a case, only a self-certification shall be obtained;

ii. Additionally, 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 the customer's registered email ID or mobile number. Further, the declared address shall be verified through positive confirmation within two months, by means such as an address verification letter, contact point verification, deliverables, etc.; and

iii. the Company may obtain a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.

The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to us the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at our end.

17. RECORD MANAGEMENT

The Company shall take the following steps regarding the maintenance and preservation of customer account information:

i. maintain all necessary records of transactions between the Company and the customer for at least five years from the date of the transaction;

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

ii. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of the business relationship, for at least five years after the business relationship is ended;

iii. make available the identification records and transaction data to the competent authorities upon request;

iv. introduce a system of maintaining proper records of transactions prescribed under rule 3 of the Rules; and

v. the documents or records maintained shall have the following information:

a. nature of the transaction;

b. amount of the transaction;

c. the date on which the transaction was conducted; and

d. the parties involved in the transaction.

18. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

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

B. The Company shall endeavor to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

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

19. REVIEW AND MODIFICATION

The Board shall review and recommend amendments to this Policy on an annual basis and as and when there is an update in the applicable laws in this regard.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

ANNEX 1

DIGITAL KYC PROCESS

Section A - Customer Information

1. The Company shall have an application or subscribe to a third-party application for carrying out customer on-boarding process and to collect such minimal information that may be required to showcase available loan products.

2. The access of the application shall be controlled by the Company and it should be ensured that the same is not used by unauthorized persons. The customer application shall be accessed through registered mobile number, live one time password and additional device based biometric authentication (2FA) followed by their E-mail ID verification with one time password.

3. The customer, for the purpose of KYC, shall provide/upload PAN details, bank account details, AADHAR and such other information that may be required through the application.

4. The live photograph of the customer along with his location shall be captured by the customer through the application.

5. The application of the Company shall have the feature that only a live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing the live photograph should be plain and no other person shall come into the frame while capturing the live photograph of the customer. One time permission shall be taken to capture the live photograph and location.

Section B - KYC Verification

6. The company's executive shall validate his credentials through an OTP to be confirmed in the customer's application. Upon validation, the customer consents for verification of his/her KYC details by the company.

7. The CKYC process is initiated with the registered mobile number and OTP validation via UIDAI's licensed Aadhaar authentication partner is carried out. CKYC fetch attempted from CERSAI with OTP from Customer. If CKYC record is found: a.) XML file parsed to extract name, DOB, address,

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com

document type, image, etc. b.) Data stored in encrypted format in Tenmark systems. c.) CKYC KIN (KYC Identification Number) stored.

8. If CKYC validation is not successful, then the company shall re-direct the customer on the application to UIDAI-licensed DigiLocker interface. Aadhaar-linked XML with masked Aadhaar is retrieved using DigiLocker credentials. Name, DOB, photo, address, and reference ID are extracted and validated. Aadhaar masked version is retained; full Aadhaar number is not stored and Signed XML hash is retained for auditability.

9. If both CKYC and Digilocker validation is not successful, then the customer enters AADHAR number manually to verify his KYC though an OTP sent to his registered mobile number via UIDAI gateway (via registered KUA). Consent-based masking logic is used to retain only the last 4 digits of AADHAR and full AADHAR is not stored.

10. On successful verification of KYC, the customer is directed to the loan process flow. If the KYC validation is not successful, the customer's loan application journey will be concluded.

11. After the KYC verification is completed, PAN validation is performed using the NSDL API, including status and name matching.

12. As part of the loan process flow, upon the loan application being submitted, the company carries out screening of the customer's name against the UN sanctions list, RBI defaulters list and Internal fraud watchlists before approving the loan application.

Note: No document images (Aadhaar, PAN front/back) are uploaded by the customer at any stage. All data is system-fetched and logged via APIs.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033
+91-6384600199 compliance@tenmarkcapital.com

ANNEX 2

ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS

1. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
2. Unnecessarily complex client structure.
3. Individual or classes of transactions that take place outside the established business profile and expected activities/ transaction unclear.
4. Customer is reluctant to provide information, data, documents;
5. Submission of false documents, data, purpose of loan, details of accounts;
6. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds are doubtful etc.;
7. Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
8. Approaches a branch/ office of TCPL, which is away from the customer's residential, or business address provided in the loan application, when there is a branch/ office nearer to the given address;
9. Unable to explain or satisfy the numerous transfers in account/ multiple accounts;
10. Initial contribution made through unrelated third-party accounts without proper justification;
11. Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount;
12. Suggesting dubious means for the sanction of loan;
13. Where transactions do not make economic sense;
14. Unusual financial transactions with unknown source.
15. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
16. There are reasonable doubts over the real beneficiary of the loan;
17. Encashment of loan amount by opening a fictitious bank account;
18. Applying for a loan knowing fully well that the property/dwelling unit to be financed has been funded earlier and that the same is outstanding;
19. Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
20. Multiple funding of the same property/dwelling unit;
21. Request for payment made in favour of a third party who has no relation to the transaction;
22. Usage of loan amount by the customer in connivance with the vendor/builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated.
23. Multiple funding / financing involving NCO / Charitable Organisation / Small/ Medium Establishments (SMEs) / Self Help Croups (SHCs) / Micro Finance Croups (MFCs)
24. Frequent requests for change of address;
25. Overpayment of instalments with a request to refund the overpaid amount.
26. Investment in real estate at a higher/lower price than expected.
27. Clients incorporated in countries that permit bearer shares.

Registered Office: 12/1 (10/1), Varadappan Street West Mambalam, Chennai - 600033

+91-6384600199 compliance@tenmarkcapital.com