POLICY ON KNOW YOUR CUSTOMER

&

ANTI-MONEY LAUNDERING ("AML") MEASURES

Digamber Capfin Limited

Document Control Page

Document Name	:	**Digamber Capfin Limited – Policy on Know Your Customer & Anti-Money Laundering ("AML") Measures**

Document Owner	:	**Compliance Department-Digamber Capfin Limited**
Reviewed By	:	**Board of Directors**
Approved By	:	**Board of Directors**

Classification	:	**Internal Use Only**
Distribution List	:	**Digamber Capfin Limited**

Revision History	
Dates	**Status**
10.07.2017	**Approved**
31.03.2018	**Reviewed**
24.08.2019	**Reviewed**
05.09.2020	**Reviewed**
24.08.2021	**Reviewed**
26.03.2022	**Amended**
26.05.2022	**Reviewed**
09.02.2024	**Reviewed**
21.08.2024	**Amended**
03.01.2026 (Adjourned meeting held on 29.12.2025)	**Amended**

Table of Contents

1. INTRODUCTION

Reserve Bank of India, one of the regulatory agencies entrusted with the responsibility of driving the anti-money laundering initiatives advised NBFCs to follow certain customer identification procedure for opening of accounts and monitoring transactions of suspicious nature for the purpose of reporting it to appropriate authority. RBI revisited these guidelines from time to time keeping in view the recommendations of Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism.

Reserve Bank of India (RBI) has issued Master Direction - 'Know Your Customer' (KYC) Direction 2016,RBI/DBR/2015-16/18 DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25th, 2016 as amended from time to time thereby setting standards in terms of provisions of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 as amended from time to time by the Government of India.

The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this policy to confirm to the standards so prescribed. This policy is applicable across all branches / business segments of the company, and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which shall be advised by RBI from time to time.

The Company endeavours to frame a proper policy framework on 'Know Your Customer' (KYC) and Anti- Money Laundering measures as per Master Direction – Know Your Customer (KYC) Directions, 2016 as may be issued and amended by Reserve Bank of India from time to time. The Company shall make all the relevant changes/amendments/insertions in this Policy whenever required and will review it as per said directions. The Company is committed for transparency and fairness in dealing with all stakeholders and in ensuring adherence to provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India and all laws and regulations.

The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulges any details thereof for cross selling or any other purposes. The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his /her consent.

The company shall also communicate its KYC norms to its customers. The company shall ensure that the implementation of the KYC norms is the responsibility of the entire organisation.

The company's Board of Directors and the management team are responsible for implementing the KYC norms hereinafter detailed, and also to ensure that its operations reflect its initiatives to prevent money laundering activities.

The Company is a regulated entity and is licensed by the Reserve Bank of India ("RBI")as NBFC-MFI and through this Policy secures the compliances of the Master Direction on KYC issued and amended by the RBI from time to time.

2. OBJECTIVE

The objective of this Policy is to prevent the Company being a NBFCs for being used, intentionally or unintentionally, by criminal elements for money laundering activities. The Policy also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business etc. which in turn help the company to manage its risk prudently. Accordingly, the main objective of this policy is to enable the company to have positive identification of its customers.

3. SCOPE

The Policy is applicable to various stakeholders including employees and customers of the Company.

4. DEFINITIONS

Terms bearing meaning assigned in terms of 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;

ii. "Act" and "Rules" means 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. "Customer" for this purpose of this Policy would have the same meaning as assigned to it under the RBI's Guidelines on 'Know your customer' and Anti-Money Laundering Measures, as amended from time to time.

v. "Certified Copy" - Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be

carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.

vi. "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;

vii. "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 include:

a. The Managing Director or a whole-time Director, duly authorized by the Board of Directors.

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

viii. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Company as per the provisions contained in the Act;

ix. "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;

x. "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;

xi. "Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry;

xii. "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 MNREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.
Provided that;

A. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India;

B. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address: -

i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
ii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iii. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.

C. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above;

D. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiii. "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;

xiv. "Person" has the same meaning assigned in the Act and includes:
a. an individual;
b. a Hindu undivided family;
c. a company a company;
d. a firm;
e. an association of persons or a body of individuals, whether incorporated or not;
f. every artificial juridical person, not falling within any one of the above persons (a toe), and

g. Any agency, office or branch owned or controlled by any of the above persons (a to f).

xv. "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.

xvi. "Principal Officer" means an officer nominated by the company, responsible for furnishing information as per rule 8 of the Rules;

xvii. "Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

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

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

xviii. "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.

Xix. People with disabilities and People with special needs especially technologically challenged ones:

The Company shall not deny any services or product to any person who is disabled whether physically or whether technological on the basis of their disabilities. Provided they are fulfilling other parameters to avail the loan from the company including their income criteria, activities/business undertaken by them, reference check, Credit score ,screening from CFT point of view, risk categorization, Obtaining of KYC documents and Form 60 or PAN and checking whether Politically Exposed Person or not etc.

The Company shall provide training to its employees to handle such cases where a person is disabled including technology disabled and they cannot complete their e-KYC.

In case the customer is technology challenged due to various restraints like education, background etc., the company shall make all possible efforts to on board the customer.

Since the company is not using any B2C app while on boarding the customer therefore a process shall be put in place where the field staff of the company shall on board the customer in the presence of any one person of his/her family who can understand the technology and each and every point is explained in detail to the customer and only thereafter the consent is taken.

5. KNOW YOUR CUSTOMER STANDARDS

The Company frames its KYC policies incorporating the following key elements:

a) Customer Acceptance Policy;
b) Risk Categorization and Management;
c) Customer Identification Procedures (CIP);
d) Money Laundering and Terrorist Financing Risk Assessment;
e) Customer Due Diligence (CDD) Procedure;
f) Record Management;
g) Reporting Requirements to Financial Intelligence Unit – India;
h) Monitoring and screening of Transactions
i) Other miscellaneous areas

6. APPOINTMENT OF DESIGNATED DIRECTOR

"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 Company shall designate a person as a 'Designated Director' to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

7. APPOINTMENT OF PRINCIPAL OFFICER

The Principal Officer shall be responsible for ensuring furnishing information as required under the Rules. The Company will designate a person as Principal Officer.

The name, designation and address of the Principal Officer shall be communicated to the FIU-IND. Similarly the company will also designate a person as alternate PO who will undertake all the works of PO in absence of PO.

8. COMPLIANCE OF KYC POLICY

a. Company shall ensure compliance with KYC Policy through:

   (i) Senior Management shall mean Whole Time Director, Chief Finance Officer, Managing Director, Chief Compliance Officer, Vice President & Chief Business Officer"

   (ii) Implementation of KYC policy by Chief Compliance officer.

   (iii) Chief Compliance Officer shall report to Whole- Time Director & Chief Finance Officer, Managing Director & Audit Committee on quarterly basis

   (iv) Review of Policy shall be done by the Board of Directors

   (v) Independent evaluation of the compliance functions of DCL policies and procedures, including legal and regulatory requirements.

   (vi) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.

   (vii) Submission of quarterly audit notes and compliance to the Audit Committee.

b. Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

a) Customer Acceptance Policy

Company's Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers.

The guidelines in respect of the customer relationship with the company broadly are detailed below:

a) No account is opened in anonymous or fictitious/benami name(s)/entity(ies);

b) No account is to be opened where the company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer;

c) No transaction or account-based relationship is undertaken without following the CDD procedure;

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified;

e) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened;

f) The company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a company desires to open another account with us, there shall be no need for a fresh CDD exercise;

g) CDD Procedure is followed for all the joint account holders, while opening a joint account if any ;

h) Circumstances, in which a customer is permitted to act on behalf of another person/ entity shall be clearly spelt out;

i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India;

j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority;

k) 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;

l) Where GST details are available, the GST number shall be verified from search/ verification facility of the Issuing Authority.

m) Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

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

b) Risk Management

For Risk Management, the Company will have a risk-based approach which includes the following:

a) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company;

b) Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in;

The above mentioned categorization shall depend and vary as per the score received from Credit Rating agencies.

Although the prospective customers of the Company are from the lower economic strata of the society and hence, they are treated as low risk clients, the Company is required to ensure overall compliance with the RBI Directions relating to KYC AML CFT requirements while doing risk categorization for its customers.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

FATF Public Statement, the reports and guidance notes on KYC/AML issued by Indian Banks Association (IBA) and other agencies, etc., may also be used in risk assessment.

c) 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) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;

(c) When company has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand;

(d) Selling third party products as agents, selling their own products and any other product for more than rupees fifty thousand.

(e) The company shall ensure that introduction is not to be sought while opening accounts.

(a) General

As required under the RBI Directions, the Company shall ensure compliance with the following processes regarding customer identification and acceptance in accordance with the applicable provisions of Aadhaar Act, 2016 and Regulations made thereunder with respect to authentication, offline verification, digital KYC, Video Based Customer Identification Process (VCIP), KYC Identifier allotted by the CKYCR or such other forms of verification of Aadhaar number or such other permissible OVDs, as may be made permissible to the Company, from time to time.

PEP declaration will also be obtained from the customer and enhanced due diligence will be undertaken wherever the customer is found PEP.

As part of the customer acceptance process, branches need to procure the following documents:

(i) Photograph of customer along with spouse, if applicable.

(ii) Prescribed KYC documents of the customer, provided the customer voluntarily provides his Aadhaar number, wherever applicable, either in physical or electronic form, for authentication or offline verification digital KYC, Video Based Customer Identification Process (VCIP), KYC Identifier allotted by the CKYCR an explicit consent to download records from CKYCR; and, or in such other form or in such manner as may be specified by the Regulations under the Aadhaar Act, 2016, as amended from time to time, as detailed below:

A digital / photocopy of any one of the following photo IDs:

First Preference:

- Proof of possession of Aadhaar Number
- Voters ID

Others:

- Driving License
- Passport
- Job card issued by NREGA duly signed by an officer of the State Government
- Letter issued by the National Population Register containing details of name and address.

A copy of any one of the following documents as address proof:

- Aadhaar Card
- Voter ID
- Driving License
- Passport
- Job card issued by NREGA duly signed by an officer of the State Government
- Letter issued by the National Population Register containing details of name and address.

Where the above documents furnished by the customer does not have updated current address, the following documents may be collected for the limited purpose of proof of address :-

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
- Property or Municipal tax receipt.
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings if they contain the address.
- 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.

The customer should submit the updated KYC documents with current address within a period of three months of submitting the documents specified above.

(i) Both Photo ID and address proof should be verified with the original and a digital image of the same should be captured by the Field Officer in respective digital applications

(ii) In case digital copies are obtained, the company official should submit an undertaking after verifying with the original and affixing the branch seal. The undertaking should be signed by the customer as well.

(iii) In case photocopies are obtained, both photo ID and address proof (photocopies) should be signed by the customer as self-attestation. Further it should be duly attested by the company official after verifying with the original and affixing the branch seal.

(iv) The Photo ID and Age proof is to be collected for spouse of the customer. This must be taken at the time of enrolment for new customers.

(v) In all cases where the Company has already obtained valid KYC documents from the customers, there is no need to obtain fresh set of documents from them if there is no change in it, while giving fresh/top-up loans.

The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 shall be obtained from the customers.

(b) Enhanced due diligence for customers other than "Low Risk" customers:

(i) the identity of the person shall have been verified before accepting him/her as a customer.
(ii) the decision to open an account is taken at a senior level in accordance with the Customer Acceptance guidelines.
(iii) all such accounts are subjected to enhanced monitoring on an on-going basis.
(iv) in the event of an existing customer or the beneficial owner of an existing account subsequently categorised as "High-Risk", senior management's approval is obtained to continue the business relationship.
(v) enhanced monitoring on an on-going basis.

In cases where any of the customers are found to be Medium/High-Risk, including their relatives or the beneficial interests in their accounts are held by persons other than the customers themselves, then the Company shall carry out enhanced due diligence procedures prescribed under applicable RBI Directions to gather sufficient information including information about the sources of funds, accounts of family members and close relatives.

In addition, the Company shall ensure following measures with respect to "High Risk" customers:

(c) Prohibited List of Individuals/Entities:

(i) The "ISIL (Da'esh) & Al-Qaeda Sanctions List:

https://scsanctions.un.org/ohz5jen-al-qaida.html

(ii) The "Taliban Sanctions List":

https://scsanctions.un.org/3ppp1en-taliban.htm

The Company shall ensure that in terms of Section 51A of Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, any of the existing or new customers are not in the prohibited list of individuals and entities which are periodically prescribed by local regulator from time to time. Compliance monitoring of such individuals / entities are done periodically be screening them against the below lists provided under RBI Directions as amended from time to time:

https://scsanctions.un.org/ohz5jen-al-qaida.html

Pursuant to the above screening, if any of the accounts of customers of individuals or entities are categorised as 'High-Risk', then the Company shall follow the enhanced due diligence procedures prescribed under RBI Directions. The details of such accounts shall be provided to the senior management official.

d) Money Laundering and Terrorist Financing Risk Assessment

(i) The company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise quarterly 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.

The assessment process should 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, company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time;

(ii) The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually;

(iii) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

(iv) The company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, company shall monitor the implementation of the controls and enhance them if necessary.

(v) Accordingly, the below mentioned priority areas for addressing the threats and vulnerabilities of Money laundering/Terrorists Financing risk in NBFC Sector shall be carried out while carrying out internal ML/TF Risk assessment: -

a. Effectiveness of Suspicious Activity Monitoring and Reporting

b. Availability and Access to Beneficial Ownership information

c. Effectiveness of Compliance Function (Organization)

d. Integrity of Business/Institution Staff

e) Customer Due Diligence (CDD) Procedure

Customer due diligence (CDD) Procedure in case of Individuals:

CDD is being undertaken on the basis of KYC Process as well as while assessing income and eligibility of Loans for the borrowers and her household including spouse and unmarried children. Wherever required, Enhanced Due Diligence (EDD) by way of additional OVD and information will be conducted.
Cases where EDD will be done:
a) In case the borrower is a PEP or is a relative of PEP.
b) Where the OVD taken is not clear or is old

On-going Due Diligence

The company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

Updation / Periodic Updation of KYC

The company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation.

a) Individuals:
(i) No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained

through customer's email-id registered with the company , customer's mobile number registered with the company , letter, etc.

(ii) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the company, customer's mobile number registered with the company, letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

Further, the company, at its option, may obtain a copy of OVD or deemed OVD, as defined in Section 3(a)(xiv), or the equivalent e-documents thereof, as defined in Section 3(a)(x), for the purpose of proof of address, declared by the customer at the time of periodic updation.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Additional Measures :-

In addition to the above, the company shall ensure that,

(i) The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the company are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the company has expired at the time of periodic updation of KYC, company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer

(ii) Customer's PAN details, if available with the company, is verified from the database of the issuing authority at the time of periodic updation of KYC.

(iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the company and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

(iv) In order to ensure customer convenience, the company may consider making available the facility of periodic updation of KYC at any branch.

(v) Company shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the company such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers.

c) 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 the company 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 company's end. The Ultimate responsibility of updation of KYC records (wherever required) will be of company and not of the borrower.

f) Record Management

The Company shall maintain appropriate documentation on their customer relationships and transactions to enable reconstruction of any transaction. The records shall be maintained for a period of five years from the date of cessation of the transaction. Records shall be maintained in a manner, which facilitates its easy retrieval as and when required.

g) Periodic Review and Assessment, Compliance Monitoring, Risk Management

Internal Audit department shall periodically evaluate and assess adherence to the prescribed processes and procedures with respect to KYC-AML-CFT requirements, unusual and potentially suspicious activities covering financial transactions with customers.

The Internal Audit department would also provide an independent evaluation of compliance with the applicable RBI Directions, Act, the Rules. Internal Audit would verify the application of KYC-AML-CFT procedures at the branches during every branch/Regional processing Centre audit and comment on the lapses observed in this regard.

The Internal Audit department may also take the help of external agencies, wherever required, to assess, monitor, evaluate and report any suspicious transactions relating to AML-KYC-CFT requirements, high-risk individuals/entities, PEPs, or such other prohibited individuals/entities from time to time, with the prior approval of Managing Director and/or WTD-CFO of the Company.

The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly basis.

Customer Education:

Customers would be trained on the necessity and importance of KYC document during Compulsory Group Training. Apart from these regular awareness activities shall be undertaken through other modes.

Suspicious Transaction Report (STR):

The Company shall ensure to file STR with FIU-IND in respect of following transactions:

(i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency.

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds Rupees Ten Lakhs or its equivalent in foreign currency.

(iii) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions.

(iv) All suspicious transactions whether made in cash and in manner as mentioned in the Act and Rules.

An indicative list of Suspicious Activities are provided under Annexure I.

h) Monitoring of Transactions

(i) Secrecy Obligations and Sharing of Information:

a) Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship with the customer;

b) Information collected from customers for the purpose of opening of account/proving loan shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer

c) 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 company requires disclosure and
d. Where the disclosure is made with the express or implied consent of the customer.

d) Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

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

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

(b) In terms of provision of Rule 9(1A) of PML Rules, the REs shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(d) Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

(e) As per the communique having reference no. CKYC/2022/02 dated January 20, 2022 exemption has been provided by Government of India to the companies registered with CERSAI (CKYCRR), that they are not required to upload the KYC records related to Self Help Groups (SHGs) and Joint Liability Groups (JLGs) to CKYC Records Registry.

(iii) Period for presenting payment instruments:

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

(iv) Unique Customer Identification Code (UCIC):

(a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by the company;
(b) The company shall, at their option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured

that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

(v) Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to company, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof

(vi) Hiring of Employees and Employee training

a) Adequate screening mechanism as an integral part of personnel recruitment/hiring process shall be put in place;

b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT 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 AML/CFT policies of the Company, regulation and related issues shall be ensured.

c) The Company shall, as an integral part of its personnel recruitment/ hiring process, ensure for adequate screening of individuals while hiring of employees. The basic training undertaken for each new loan officer and regular refresher training conducted at branches would ensure that field staff are adequately trained in KYC, AML and CFT procedures. Management shall review the training adequacy at regular intervals.

(vii) Adherence to Know Your Customer (KYC) guidelines by NBFCs/RNBCs and persons authorised by NBFCs/RNBCs including brokers/agents etc.

a) Persons authorised by Company for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to Company;

b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by Company including brokers/agents etc. who are operating on their behalf;

The books of accounts of persons authorised by Company including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

9. ACCESSIBILITY AND INCLUSIVE CUSTOMER SERVICE

1. Inclusive KYC Framework

The Company shall follow an inclusive KYC approach to facilitate onboarding of customers with disabilities, special needs, or technological challenges, while ensuring compliance with applicable KYC/AML regulations.

2. Assisted KYC

Where required, the Company shall provide assisted KYC support through authorised personnel for documentation and verification, subject to regulatory permissibility.

3. Alternative Authentication

Subject to applicable regulations, alternative legally valid authentication may be accepted where customer is unable to perform the KYC and signatures and certifications through e-kyc and e-signature mode.

4. e-KYC Exceptions

Where e-KYC modes are not feasible, alternate or assisted KYC channels may be permitted. Customers shall not be denied onboarding solely due to inability to complete e-KYC independently.

5. Consent and Confidentiality

Explicit customer consent shall be obtained for assisted processes, and data privacy and confidentiality shall be maintained at all times.

6. Staff Sensitization

Relevant staff shall be sensitized on handling customers with disabilities, special needs, and assisted KYC processes

10. UPLOADING OF KYC DATA ON CERSAI PLATFORM

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR. In terms of provision of Rule 9(1A) of PML Rules, the company shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(b) The company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prescribed by CERSAI for 'Individuals' and 'Legal Entities' (LEs), as the case may be.

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

(d) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the company shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the specified dates, at the time of periodic updation or earlier, when the updated KYC information is obtained/received from the customer.

(e) the company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(f) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the company, with an explicit consent to download records from CKYCR, then the company shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless: –

(a) there is a change in the information of the client as existing in the records of Central KYC Records Registry; or

(b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the respective regulator; or

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

(d) the reporting entity considers it necessary in order to verify the identity or address (including current address) of the client as per the guidelines issued by the regulator under sub-rule (14), or to perform enhanced due diligence or to build an appropriate risk profile of the client";

If any other Regulated Entity has modified the details in CKYC for any client of the company, then within 7 days of receiving notification latest set of KYC needs to be downloaded by the company.

ANNEXURE –I

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

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

Transactions that do not make Economic Sense

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

Activities not consistent with the Customer's Business

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

Attempts to avoid Reporting/Record-keeping Requirements

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

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

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

Unusual Activities

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

Customer who provides Insufficient or Suspicious Information

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

b) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
c) A customer who has no record of past or present employment but makes frequent large transactions.

Certain NBFC Employees arousing Suspicion

a) An employee whose lavish lifestyle cannot be supported by his or her salary.
b) Negligence of employees/willful blindness is reported repeatedly.

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

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

Digamber Capfin Limited

Address: J 54-55, Anand Moti, Himmat Nagar, Gopalpura, Tonk Road, Jaipur-302018, Rajasthan.