V.4/3/24 (25-03-2024)

YOGAKSHEMAM LOAN LTD.,

KNOW YOUR CUSTOMER (KYC) POLICY

(Pursuant to the Master Direction DBR.AML.BC.No. 81/14.01.0001-2015-16 updated as on 20.04.2018)

Review History

Originally Approved	Board Meeting	28th February,2015
Review and Amended	Board Meeting	16th July,2018
Review and Amended	Board Meeting	23rd January,2021
Review and amended	Board Meeting	25th March 2024

Contents

I) Introduction

The Reserve Bank of India, (hereafter in this policy referred to as RBI) has issued on 4th January 2024 the updated direction namely Reserve Bank of India (Know Your Customer (KYC) Directions, 2016. (Hereafter in this policy referred to as the Directions). The said directions are applicable to all regulated entity which includes NBFCs as well. In terms of Para 4 of the Directions, the company shall put in place a Know Your Customer Policy (KYC) policy duly approved by the Board.

II) Scope and Coverage

Pursuant to the above Directions, this policy shall act as the guideline for compliance with the regulatory requirement of having in place a sound customer acceptance practices and prevention of money laundering using the systems of the company detriment of broad national interest of the country. The policy will cover all transactions where customer interface is involved.

III) Designated Director

1) The Board of directors of the company shall designate a director, preferably the a director in the full time employment of the company to be the Designated Director to ensure the overall compliance with the obligations of the company under the Prevention of Money Laundering Act and the Prevention of Money Laundering (Maintenance of Records) Rules 2005.
2) The particulars of the designated directors shall be communicated to FIU-IND including the changes if any in the case of the Designated Directors.
3) Additionally, the RBI will be provided with the Name, designation, address, and contact details of the Designated Director.
4) The Principal Officer cannot be nominated as the 'Designated Director' under any circumstances.

IV) Principal Officer

1) The Board shall appoint a Principal Officer who shall be responsible for ensuring compliance, monitoring transactions, and reporting as may be required under the Act and Rules.

2) The required particulars of the Principal Officer shall be communicated to FIU IND including the changes, if any, in the case of the Principal Officer.

3) Additionally, the RBI should be provided with the Principal Officer's name, designation, address, and contact details.

V) Compliance of KYC Policy

1) The senior management team members of the company shall ensure that the KYC process and procedures prevailing in the company across the applicable segments are in compliance with this policy.

   Explanation; senior management for the purpose of this policy includes all business heads in charge of different loan portfolios and liability products of the company existing as on the date of the notification of this policy and brought into existence hereafter.

2) The effectiveness of compliance with the policy shall be ensured through proper systems and controls including installation of computer software.

3) The scope of internal inspection wing of the company and the internal auditors on contract shall cover the review of effectiveness of the policy and reports shall be put up to the Audit committee on a quarterly basis.

4) Wherever the company is availing the services of third parties for business solicitation or sourcing of customers such as engagement of Direct Sales Agents, including fin-tech companies, startups or loan aggregators, the outsourced arrangements shall not compromise the companies power to accept or reject a customer based on KYC compliance. The KYC compliance functions shall not be outsourced.

VI) KYC policy

The KYC policy of the company will have the following elements

A. Customer Acceptance Policy
B. Risk Management
C. Customer Identification Procedure(CIP) and
D. Monitoring of Transactions.

A. Customer Acceptance Policy

1. Business of the Company and Acceptance of Customers

The customer acceptance of the company in relation to its business encompasses the sanctioning of credit against the security of household gold jewellery, (Gold Loans)

immovable properties (Commonly referred to as Loan Against Property (LAP), automobiles and plant and machineries, unsecured loans to traders and service providers, micro finance, money transfer agency business and also the mobilization of resources from retail individuals by way of issue of Non-Convertible Debentures (NCDs) and subordinated debt.

The company is committed to accept customers without any discrimination either for an account based relationship or as a walk in customer across its branches/ other place of business subject to;

i. Whose identity is established
ii. Who is not carrying on any illegal activity
iii. Who has not been notified as a high risk customer by any national or international agency included in the sanctioned list or as part of any international treaty to which India is also a party.

2. Principles for customer acceptance

a. While accepting a customer for an account based transaction or otherwise, the company will not open accounts or permit transactions in anonymous / fictitious/benami names.
b. Where the company is not able to carry out the Customer Due Diligence (CDD) measure whether on account of deficiencies in the documents or information provided to it by the customer or on his non-cooperative approach, the company will not facilitate the opening of an account or a transaction in its branches or other place of business.
c. In the case of Gold Loans, considering the very nature of the loans, the small ticket size and the gold loans are generally availed for a duration up to one year and that it is fully secured, the company will adopt a simplified KYC process of identifying the customers with the proof of identity and address in the normal course.
d. In cases where the exposure to a gold loan customer exceeds certain threshold and identified as high value transactions as a risk mitigation measure, a detailed customer due diligence shall be carried as prescribed in this policy.
e. In case of other loans, the customer acceptance shall be subject to detailed CDD.

f. The customer acceptance in respect of mobilisation of resources from individuals or legal entities by the issue of NCDs and subordinated debt shall be subject to KYC compliance and all the transactions shall be through banking channels.

g. Mandatory documents/ information for the purpose of complying with its KYC requirement shall be as detailed in the following pages of this policy. KYC documents shall be updated by the company on a periodic basis as provided herein.

h. vii. Wherever the company is obtaining any additional information from the customers after opening the account as part of its CDD process, it shall be done with the express consent of the customer and the company shall record the consent either physically or digitally.

i. The company shall allocate a Unique Customer Identification Code (UCIC) for each customer and all relationship with the company shall be mapped to this code. The CDD process shall be ensured at the UCIC level such that it need not be repeated for further transactions of the customer for each time he opt for an account based transaction or otherwise.

j. While opening joint accounts, the CDD procedure shall be followed for all the joint applicants.

k. The company may accept a person representing a legal entity subject to proper and valid authorisation from the entity of which he represents subject to compliance with KYC requirements. It also accept a person in place of another person in circumstances of death, permanent or temporary incapacity, or permanent relocation of the later. The acceptance of the other person shall be subject to proper, authorisation, records of inheritance and KYC compliance.

As a policy the company will not deny banking facility to the general public especially those, who are financially or socially disadvantaged subject to the other provisions of this policy.

B. Risk Management

i. The company shall have a risk based approach while on boarding customers.

ii. Since the company is predominantly carrying on the business of loan against the security of house hold gold jewellery, the risk perception on customers with normally accepted KYC documents are considered to be in the low risk category. However, for the purpose of closer monitoring an exposure based risk categorization is adopted. For

Gold loans *customers* with an exposure limit up to Rs.10.lacs will be considered as low risk subject to a domicile distance of 10.kms radios of its branches. (Domicile for this purpose includes his place of business as well). Rs.10.lacs to Rs.50.lacs with a distance up to 25 kms will be considered as Medium risk and above that limit will be classified as High risk

iii. In respect of CDD process, customers having KYC documents such as Aadhaar and PAN, which can be authenticated in the online will be categorized as low risk customers. While customers having OVDs without PAN will be classified as medium risk and those do not have any of the OVDs, politically exposed persons, people having criminal back ground, carrying on business which is prohibited under any law, or having business located in a high risk jurisdiction/facing international sanctions etc. will be categorized as high risk. The company should not in the ordinary course deal with people or organisations notified by the Finanical Action Task Fource,RBI or other regulatory bodies of the Government.

iv. The company may collect information on its customers from multiple sources in a non- intrusive manner.

v. Money Laundering and Terrorist Financing Risk Assessment:

a. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, 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. Considering the size of the Company, scale of its operations and nature of activities, the customer identification process and the due diligence process itself take care of the risk in this respect as generally the customers are from the local limit of the branches and the business consists only of distribution of loans to residents. However,while preparing the internal risk assessment, it it shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company.

b. 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 audit committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

c. The outcome of the exercise shall be put up to the Board as reviewed and recommended by the audit Committee, and should be available to competent authorities and self-regulating bodies. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. The Company shall implement a CDD program, having regard to the ML/TF risks identified and the size of business. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

3. PML ACT, 2002

Prevention of Money Laundering Act, 2002 (PMLA) was enacted to fight against the criminal offence of legalizing the income/profits from an illegal source. The Prevention of Money Laundering Act, 2002 enables the Government or the public authority to confiscate the property earned from the illegally gained proceeds. The PMLA seeks to combat money laundering in India and has three main objectives: To prevent and control money laundering. To confiscate and seize the property obtained from the laundered money; and. To deal with any other issue connected with money laundering in India. At the Company level, suitable internal policies and controls are to be installed to ensure that its systems are not targeted as conduits for money laundering.

C. Customer Identification Procedure (CIP)

1. Customer Identification means the process of customer due diligence whereby the identity of the customer and the beneficial owner is verified.

The company shall undertake identification of customers in the following cases:

a) Commencement of an account-based relationship with the customer.
b) Carrying out transactions for a non-account based customer, that is a walk-in customer, (like money transfer)where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or

several transactions that appear to be connected. Further it shall also do a CDD where it appears that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

2. Subject to the regulations issued by the RBI from time to time the company may avail the services of third party service providers for the purpose of verifying the identity of customers at the time of commencement of an account-based relationship subject to the following conditions:

   i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
   ii. The company shall take adequate steps to ensure that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
   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 PML Act.
   iv. The third party shall not be based in a country or jurisdiction assessed as high risk.

D. Monitoring of transactions

a) The photo of the customer which is already being captured at the time of creation of Customer ID file shall be continued.

b) Photocopy of the KYC document submitted by the customer shall be countersigned by the customer and signed by the BM/BH/ABH after comparing with the original document. It shall also contain the Customer ID number and shall be filed carefully for future verification.

c) In case of customers whose accounts have not been operated (or who have not been transacting) for more than 12 months fresh KYC documents will need to be taken before undertaking any new transactions. System based control will be put in place.

d) Accounts in the names of individuals having a track record of criminal offence, if in the knowledge of the branch/company, should not be opened under any circumstances. Further, the system should block the opening of accounts in the names of individuals / organizations engaged in activities which are illegal (e.g. terrorism) and circulated by the United Nations.

e) On- going due diligence: - given the nature of gold loans, the company shall undertake continued due diligence of customers to ensure that their transactions are consistent with knowledge of the company about the customers and the risk profile.

f) Periodic updation:-The Company shall update the KYC document once in two years in respect of customers classified as high-risk and in other cases it may be verified once in three years . It shall be done in the following manner;

i. PAN shall be verified with the issuing authority.

i. Aadhaar shall be authenticated with the explicit consent of the customer.

ii. In case the Aadhaar does not have the current address an OVD containing current address shall be obtained.

g) The records regarding the customer identification and of the transactions with the customers and the company shall be properly maintained in accordance with the provisions of applicable law and shall be retrievable at least for a period of five years from the date of transactions.

h) Reporting:- The company shall report to the Financial Intelligence Unit- India (FIU-IND) cash transactions and of suspicious transactions as per the requirement under the Prevention of Money Laundering (Maintenance of Records) Rules ,2005.

i) Maintenance of privacy: - The Company shall put in place proper mechanism for the preservation of personal information and KYC documents the sharing of information shall be on a need to know basis only.

Explanation;Financial Intelligence Unit - India (FIU-IND) is the central, national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions to enforcement agencies and foreign FIUs

VII. Customer Due Diligence (CDD) procedure

The Customer Due Diligence Procedure commences with the collection of KYC documents. The Company will broadly follow the KYC norms guidelines as applicable for NBFCs issued by the Reserve Bank of India. This will include reporting of cash transactions, suspicious transactions, blocking accounts in the names of banned entities; persons with criminal background etc. as advised vide RBI instructions from time to time.

A. Individuals/ Natural persons

Establishing the Identity and Address of the customer is key to the CDD. The company shall follow the following methods for effective CDD in case of individuals;

1. In respect of an individual the following shall be obtained;
   i. PAN or Form -60
   ii. Capturing of live photograph/One recent Photograph and
   iii. A certified copy of an Officially Valid Document (OVD) containing the identity and address of the individual.

Provided that in case the OVD submitted by 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.

B. Officially Valid Documents for the purpose mean and includes all or any of the following*;*

1. Passport
2. Driving license,
3. Voter's Identity Card issued by the Election Commission of India,
4. Job Card issued by NREGA duly signed by an Officer of the State Government,
5. National Population Register Containing details of name and address.
6.Adhar/ proof of possession of adhar number

C. KYC document for individuals shall comprise of 2 aspects viz

(i) Proof of Identity & (ii) Proof of Address.

Proof of Identity will carry the photograph of the holder while Proof of Address will contain the present address of the customer.

The prima facie genuineness of both the documents must be verified by the branch staff.

Some documents may serve as both Proof of Identity and Proof of Address, but in such cases

it must be ensured that the document mentions the present/current address of the customer otherwise a separate Proof of Address will be required.

i. **IDENTITY** : Common documents evidencing Proof of Identity
   Passport.
   PAN Card.
   Voter ID Card.
   Driving licence.
   Ration Card with photo.
   UIDAI card (Aadhaar).
   All the above documents except PAN card could serve as Proof of address also provided they contain the current valid address.

ii. **ADDRESS**: Common documents evidencing Proof of Address
   Telephone bill.
   Electricity bill.
   Water bill.
   Bank account / Credit card statement.
   Municipal / Local/House tax bill / receipt.
   Authentic rent receipt / lease document.
   Letter from reputed employer, public authority.
   {*In case the customer is staying with a close relative such as husband, wife, son etc. Proof of Address in the name of the close relative may be accepted provided a certificate / letter is obtained from the close relative that the customer (name) is staying with him/her*}

iii. 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 indicated in Chapter IX of the Master Direction (MD).

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

v. 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 (21 of 2000).

D. KYC FOR NON-INDIVIDUALS (COMPANIES, FIRMS, TRUSTS ETC.)

KYC norms are applicable to non-individuals also. The requirements are as under.

Companies Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.	Certificate of incorporation with Memorandum & Articles of Association. Resolution of Board of Directors for opening the account and authorization of persons to operate the account. PAN allotment letter. Copy of telephone bill Copy of Aadhaar or OVD and PAN of the Persons entitled to 10% or more of the equity capital/ or voting rights (Beneficial Owners) Copy of Aadhaar or OVD and PAN of the persons authorized to operate the account on behalf of the company.
Partnership Firms Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.	Registration certificate, if registered Partnership Deed Power of attorney authorizing a partner / employee to carry out transactions on behalf of the firm Valid documents identifying the partners / Power of Attorney holders (same as applicable for individuals as mentioned in para 3 (ii) CDD procedure above) Telephone bill in the name of the firm / partners
Proprietorship Firms	Valid documents identifying the proprietor (same as applicable for individuals as mentioned in para 3(ii) above) PLUS (*any two of the below mentioned documents*) Registration certificate, if registered

	Certificate /Licence issued under Shops & Establishment Act GST / Income Tax returns VAT / CST registration Licence issued by Govt / Autonomous /Regulatory Bodies Utility bills of Electricity, water, land line telephone bills
Trusts , Associations	Certificate of registration if registered Power of attorney authorizing a person to carry out transactions on behalf of the trust Valid documents identifying the trustees, beneficiaries, power of attorney holder etc. (same as applicable for individuals as mentioned in para 3(ii) above) Resolution of the managing body of the trust / association Telephone bill

As a policy Gold loans will be granted to individuals/HUFs only and not to companies, firms, trusts etc.

i) In case of high value gold loan customers (above Rs. 10 .lacs) and other loan products, in addition to KYC compliance, detailed customer profiling such as verification of residence, employment or profession of the borrower shall be carried out and the management shall issue internal guidelines in this respect.

iiv) In case of gold loans the photographs of the customers shall be captured at the time of registration of KYC and shall be updated periodically as provided in this policy.

iii) Updating KYC:- The KYC of a customer shall be re-verified and updated on the expiry of 3 years in case of continuing relationships by obtaining fresh copies of all KYC documents.

E. Digital KYC Process

The company may adopt digital KYC process as part of its customer identification and due diligence process, in such case the following procedures shall be followed :-

a. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.
b. 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 Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.
c. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice-versa. The original OVD shall be in possession of the customer.
d. The Company must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Company shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp HH:MM:SS) on the captured live photograph of the customer.
e. The Application of the Company shall have the feature that only 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 live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
f. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
g. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
h. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/eAadhaar downloaded from UIDAI where QR code is available, the details

like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

i. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in for before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

j. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

k. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

l. The authorized officer of the Company shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

m. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

F. **Other Loans, Money Transfers, Foreign Exchange & Liability Products** : KYC documents as mentioned above should be taken without exception for customers

transacting in Money Transfers, and Liability Products such as NCDs and Subordinated debt irrespective of the amounts. In respect of other loan products, in addition to the KYC compliance and customer due diligence, the customer profiling shall be carried out in accordance with the loan policy.

G. Simplified CDD for certain customers

In case a person who desires to open an account is not able to produce identification information as mentioned under Para 3 above the company may permit the opening of an account subject to the following conditions:

(a) The company shall obtain a self-attested photograph from the customer.

(b) The Branch Head and the Assistant Branch Head certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) The account shall remain operational initially for a period of twelve months, within which the customer has to furnish identification information as mentioned in para 3(ii) above.

(d) Balances in such accounts of a customer taken together shall not exceed rupees fifty thousand at any point of time.

(e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

(g) The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.

(h) This facility will be permitted in the larger interest of the society such that the under privileged is not deprived of basic credit facility and will be valid for only transactions in Gold loan and no other loans shall be granted under this scheme.

(i) KYC verification once done by one branch/office of the company shall be valid for transfer of the account to any other branch/office of the company, provided the CDD procedure has already been done for the concerned account and the same is not due for

periodic update

VIII. Regularisation of Simplified KYC : Where simplified KYC document has been taken and the outstanding equals or exceeds Rs 50,000 a "pop-up" window will be thrown up in the system for regular KYC documents. Regular KYC document shall be obtained within 30 days beyond which 'exception reports' of non-compliance will be generated.

IX. Blocking non-compliant accounts : When the prescribed regular KYC documents are not obtained and updated in the system loans exceeding Rs 1,00,000 per customer shall be blocked until the prescribed KYC documents are obtained and updated in the Customer ID file.

X. Data entry : Separate fields for entering Proof of Identity, Proof of Address and simplified KYC document will be available in the Customer ID file in the system. In case of Gold loans, the live photos of the customer shall be captured and stored in the system at the time of the customer registration and the photo shall be mapped with the unique customer ID along with other KYC documents. The company may provide facility for printing the photograph in the pledge form. In case of other loans/ transactions a copy of the passport size photo of the borrower/ co-obligants to be collected as part of the CDD

XI. Women Customers: In the case of 'parda' (veil) wearing ladies capturing of the customer's photograph (in Customer ID file on the system) may waived provided an acceptable Proof Of Identity document is furnished. Photo of the customer in the Customer ID File should be obtained in all other accounts without exception.

XII. Certified Copy

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.

XIII. Central KYC Records Registry (CKYCR)

An entity defined under Rule 2(1) of the Maintenance of Record Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. The Company shall

establish registration with the CKYC and upload KYC records of its customers as per the regulations in place in this respect

XIV. Digital KYC

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 authorized officer of the Company as per the provisions contained in the Act.

XV. 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)

XVI. Equivalent e-document

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.

XVII. Officially Valid Document (OVD)

The 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.

XVIII E-KYC

a) The company may make use of the e-KYC facility for authentication of the Aadhaar using services of credible agencies by obtaining necessary license from UIDAI[1] if it is permissible to the company under the regulations. The authentication shall be in line with the rules and regulations of UIDAI either by biometric verification or by means of an OTP.b) In case of OTP based authentication, the account shall be opened for a maximum period of one year and the borrower account can be sanctioned for only term loan of rupees sixty thousand in a year the validation by means of biometric shall be ideally completed within 6 months of the OTP based authentication and in no case it shall extend beyond one year.

[1]Inserted on 05.08.2020

c) In case of e-kyc, the authentication shall be done with the consent of the customer obtained either in physical form or digitally.

XIX. Video based Customer Identification process.

Video based Customer Identification Process (V-CIP)": is a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this policy.

Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. i.The official of the Company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:i. Company can only carry out Offline Verification of Aadhaar for identification.

ii. Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India .The official of the Company shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

iv. The official of the Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

v. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

vi. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

vii. Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

viii. To ensure security, robustness and end to end encryption, the company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

ix. The audio-visual interaction shall be triggered from the domain of the company itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

x. Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xi. Company to take assistance of the latest available technology, including ArtificialIntelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer.

xii. RE shall ensure to redact or blackout the Aadhaar number for prevention of misuse and data protection.

XX. Record Management

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

(a) Maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of transaction;

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

(c) Make available swiftly, the identification records and transaction data to the competent authorities upon request;

(d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) The nature of the transactions;

(ii) The amount of the transaction and the currency in which it was denominated;

(iii) The date on which the transaction was conducted; and

(iv) The parties to the transaction.

(f) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

The Companies 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 Companies shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

XXI. V-CIP Infrastructure

i) The Company should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other

general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Companies exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

ii) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application

should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

XXII. Additional Measures for Aadhaar

Whenever the Company accepts Aadhaar as a document for proof of identity or address in physical mode, the following additional measures shall be adopted

a) While entering the number of Aadhar system shall facilitate the masking of Aadhaar number except the last 4 digits so that the Aadhaar number will not be visible in full
b) In case the management is desirous of retrieving the full number for any official purpose, the same shall be at a senior level functionary at the Corporate office and should be limited to users with supervisory passwords.
c) In case of physical storage of copies of Aadhaar card, the number shall be masked except the last 4 digit.

XXIII. .Secrecy Obligations and Sharing of Information:

(a)The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.

(b) Information collected from customers for the purpose of opening of account 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) While considering the requests for data/information from Government and other agencies, REs shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of the Company requires disclosure and

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

XXIV. Effective date:- The policy will be effective from the date on which it is approved by the Board of directors.

XXV. Review of Policy:- The Board may review the policy as and when it deems fit and shall be reviewed at least once in two years.

XXVI. Internal guidelines;- The management shall issue internal guidelines for the effective implementation of the policy.

XXVII. Language: - Language used in this policy in the singular form is deemed to include its plural form as well and vice versa. Similarly an expression in the masculine character also is deemed to include its feminine equivalents as well and vice versa.

.

RAJESH KUMAR K

Digitally signed by RAJESH KUMAR K
Date: 2024.06.01 14:18:57 +05'30'

****