KUHOO's Know Your Customer (KYC) Policy & Anti-Money Laundering (AML) Measures

Presented By

Kuhoo Finance Private Limited

Information:

Document	Classification	Version	Status
KYC & AML Policy	Confidential	1.0	Adopted vide resolution of the Board of Directors

Version History, Verification and Approval:

Date	Version	Description of Change	Owner	Approved By
18-11-2024	1.0	1st Policy prepared	Ganesh Shete	Shridhar Hebbar

Table of Contents

1 KUHOO Know Your Customer Policy & Anti Money Laundering Measures

1.1 Preview

The Company endeavours that the policy framework on 'Know Your Customer' (KYC) and Anti-Money Laundering measures is in consonance to the company's commitment in ensuring adherence to all laws and regulations and at the same time ensuring that it's dealing with all stakeholders are transparent and fair. The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof without the consent of the customer or as required under the applicable laws, rules, regulations and statutes as applicable from time to time.

The Company commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer will be sought separately with his / her consent and after effective rendering of services.

The employees of the Company will offer assistance, encouragement and service in a fair, equitable and consistent manner. The Company will also communicate its KYC norms to its customers by uploading the same on its website. The Company will ensure that the implementation of the KYC norms is the responsibility of the entire organisation. The Company's fair lending practices shall apply across all aspects of its operations including marketing, loan origination, processing, and servicing and collection activities. 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 shall have a Concurrent / internal audit system to verify the compliance with KYC/AML policies and procedures and shall ensure submission of audit notes and compliance to the Audit Committee on a quarterly basis.

The Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for Non Banking Finance Companies (NBFCs) thereby setting standards for prevention of money laundering activities and fair corporate practices while dealing with their customers. 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 conform 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 and regulatory guidelines issued from time to time.

The contents of the policy shall always be read in tandem / auto-corrected with the changes/modifications which may be advised by RBI from time to time.

For the purpose of KYC policy, a 'Customer' may be defined as:

1) a person or entity that maintains and /or has a business relationship with the Company;
2) one on whose behalf such relationship is maintained (i.e. the beneficial owner);
3) any person or entity connected with a financial transaction which can pose significant reputation or other risks to the company.

Senior Management for the purpose KYC compliance would include the Whole-Time Directors, CEO, COO, CFO , CBO and Principal Officer.

1.2 Objective

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

The Company has framed its KYC policies incorporating the following key elements:

1) Customer Acceptance Policy
2) Customer Identification Procedures
3) Monitoring of Transactions
4) Risk Management
5) Risk Categorisation of customer profile
6) Reporting of transactions under KYC norms
7) Customer Education
8) Appointment of Principal Officer
9) Appointment of Designated Director
10) Storage and Preservation of records.
11) Reliance on third party due diligence
12) Rules for identification of beneficial owner
13) Periodic Updation
14) Obtaining Permanent Account Number (PAN)
15) Money Laundering and Terrorist Financing Risk Assessment

1) Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) for the company are given below:

- No account is opened in anonymous or fictitious/ benami name(s).
- No account is 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. The company shall consider filing an STR with FIU-Ind, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- No transaction or account-based relationship is undertaken without following the CDD procedure.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- Additional information, where such information requirement has not been specified in the internal KYC Policy of the company , is obtained with the explicit consent of the customerWhile carrying out due diligence the company will ensure that the procedure adopted will not result in denial of services to members of the general public, especially those, who are financially or socially disadvantaged.
- For the purpose of risk categorisation of customer, company shall obtain the relevant information from the customer at the time of account opening.
- The Customer Due Diligence (CDD) procedures shall be carried out at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer desires to open another account with the Company, there shall be no need for a fresh CDD exercise.
- CDD Procedure is followed for all the joint account holders, while opening a joint account.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

2) Customer Identification Procedure (CIP)

Customer Identification Procedure is to be carried out at different stages i.e.

- While establishing a account based relationship (or)
- Where the company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any.
- When the company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information from the third party or

from the Central KYC Records Registry. The Company will obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).

Commented [KM1]: Point Re reliance on third-party for CDD missing

For undertaking Customer Due Diligence, the Company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

1. the Aadhaar number where,

Commented [KM2]: Not sure how this is relevant

a. He decides to submit his Aadhaar number voluntarily; or

b. the KYC Identifier with an explicit consent to download records from CKYCR, and

2. Offline verification

a. the proof of possession of Aadhaar number where offline verification can be carried out; or

b. the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

3. the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962, and

4. such other documents or the equivalent e-documents thereof as may be required by the Company.

Provided that where the customer has submitted,

i) Aadhaar number under clause (1) above to the company notified under first proviso to sub-section (1) of section 11A of the PML Act, company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the company

ii) the proof of possession of Aadhaar under [(2) (a)] above where offline verification can be carried out, the Company shall carry out offline verification.

iii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a "live photo" as specified under

Digital KYC Process.

iv) any OVD or proof of possession of Aadhaar number under clause [(2) (b)] above where offline verification cannot be carried out, the Company shall carry out verification through "digital KYC" as specified under Digital KYC Process.

v) KYC Identifier under clause (ac) above, the Company may retrieve the KYC records online from the CKYCR in accordance with requirements under Para 56 "CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)"

Provided that for a period not beyond such date as may be notified by the Government for a class of Companies, instead of carrying out digital KYC, the Company pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent live photograph where an equivalent e-document is not submitted.

The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the any scheme notified under section 7 of Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

The Company shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required.
The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

For customers that are legal persons or entities, the Company will (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure-I for guidance of Company.

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lender's prudence and the legal requirements as per established practices. The Company will take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in the Annexure-I. Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank of India from time to time.

Necessary checks wherever and to the extent possible, shall be conducted before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities. The documents requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Management in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

Further, the Company shall allot a Unique Customer Identification Code (UCIC) while entering into new relationships for individuals customers.

"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.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

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

"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 RE as per the provisions contained in the Act.

"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).

"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.

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

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

"Video based Customer Identification Process (V-CIP)": 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.

The Company may undertake live V-CIP to carry out

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, company shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, apart from undertaking CDD of the proprietor.

ii) Updation/Periodic updation of KYC for eligible customers

ii. The company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure and the V-CIP connection and interaction shall necessarily originate from 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 company's 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

iii. 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.

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

v. 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

vi. 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.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.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.

vi. The Company shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the RE specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon itf there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.Any prompting, observed at end of customer shall lead to rejection of the account opening process

vii. The official of the Company performing the V-CIP shall record video as well as capture live photograph of the customer present for identification and obtain the identification information using

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with Para 56 of KYC Directions, using the KYC identifier provided by the customer

d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

viii. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner

ix. The 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.

x. Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

xi. The official of the Company shall ensure that livephotograph 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.

xii. 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.

xiii. 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.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML

file / Aadhaar QR code, company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, company shall ensure that no incremental risk is added due to this.

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

xv. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

xvi.

xvii. To ensure security, robustness and end to end encryption, the Company shall carry out Vulnerability Assessment, Penetration testing and security audit and validation of the V-CIP Infrastructure and application before rolling it out. 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. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines

xviii. The audiovisual 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.

xix. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp in a system / systems located in India that affords easy historical data search.

xx. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xxi. The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of the RBI Master Direction - Know Your Customer (KYC) Direction, 2016.

Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs):
In case a person who desires to open an account is not able to produce documents, as specified in Section 16, NBFCs may at their discretion open accounts subject to the following conditions:

(a) The NBFC shall obtain a self-attested live photograph from the customer.
(b) The designated officer of the NBFC 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 CDD shall be carried out.
(d) Balances in all their accounts 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 (disbursements) 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) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per CDD

3) **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 same company, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.Monitoring of Transactions**

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk to a significant extent only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity attached with the client. The Company will pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Company may prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company. Further the Company shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations.[iii]

The Company ensures that its branches continue to maintain proper record of all cash transactions, if any. The internal monitoring system will have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the "offence of money laundering" as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

All transactions of suspicious nature shall be reported. The Principal Officer of the Company shall ensure that such reporting system is in place and shall monitor receipt of the reports. All transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority by the Principal Officer.

The necessary documents, information and records would be maintained and preserved for the period prescribed under PML Act, 2002 would be maintained.

4) **Risk Management**

The Board of Directors of the Company ensures that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company may, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers and apply various Anti-Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship. The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Internal Audit team should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The Company have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

5) **Risk Categorization of Customer Profile**

The Company shall monitor all its transactions from money laundering risk perspective, which may be unique to its products, services, distribution channels, administration and local jurisdiction, with specific attention to complex and unusually large transactions which have no apparent economic or visible lawful purpose. The Company shall periodically review profile of new and/ or existing customers against lists of prohibited individuals and entities issued by the United Nations or any other regulatory /statutory authorities. Such due diligence must be conducted based on the risk categorization of customers, as under.

Classify customers into various risk categories based on risk 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 Company will adopt, enhance, and modify the High, Medium and Low Risk Categories from time to time in compliance with applicable guidelines. Refer Annexure II for details.

6) **Reporting of transactions under KYC norms**

The Company shall report to the FIU-IND, details of the transactions /documents referred to in Clause (a) of sub-section 12 of PMLA, 2005 read with Rule 3 of Prevention of Money Laundering (Maintenance of Records of the Nature and Value of Transaction etc.) Rules 2005, as amended, from time to time. Refer Annexure II for details.

7) **Customer Education**

Implementation of KYC procedures requires the Company to demand certain information from customers which may be of personal nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company endeavours to educate the customer of the objectives of the KYC programme but at the same time ensure that the customer is not tipped off on the STR made by the Company to the FIU- IND.[vi]

8) **Appointment of Principal Officer**

The Company shall appoint a Principal Officer in accordance with the applicable KYC norms. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, reviewing the standards as set out in this KYC Policy and reporting compliance to the concerned Management/ Board/ Audit Committee, as required under the law/regulations.

The Principal Officer shall ensure that this KYC Policy is periodically reviewed and the revised policy is adopted by its Board of Directors, as recommended by the FATF and various guidelines on KYC/ AML/ CFT issued by relevant authorities from time to time[viii].

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

9) **Appointment of Designated Director**

The Company shall appoint a Designated Director (the Managing Director or a whole-time Director, duly authorized by the Board of Directors), a person designated by the Company

to ensure overall compliance with the obligations imposed under Chapter IV of the Prevention of Money Laundering Act and the Rules framed thereunder and shall be nominated by the Board.

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

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

10) **Storage and Preservation of Records**

The Company shall take the following steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of Prevention of Money Laundering Act, 2002 and Rules made thereunder:

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 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.

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.

11) **Reliance on third party due diligence**

The Reserve Bank of India has allowed that NBFCs may vide Circular No. DNBR (PD).CC. No. 005 /03.10.42/2014-15 dated December 1, 2014 to rely on a third party for the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, subject to the conditions that-

(a) the Company obtains necessary records or information of such client due diligence carried out by the third party within two days from the third party or from the Central KYC Records Registry;
(b) the Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
(c) the Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record- keeping requirements in line with the requirements and obligations under the Act;
(d) the third party is not based in a country or jurisdiction assessed as high risk; and
(e) the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.
(f) The Company will decide and prepare separate guidelines for this purpose.

12) Rules for identification of beneficial owner

The Company may follow the below rules for identification of beneficial owner:

where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means. Explanation.- For the purpose of this sub-clause-
"Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;
"Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;
where the client 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 ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;
where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than

fifteen percent of the property or capital or profits of such association or body of individuals;
where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

13) **Periodic Updation**

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 subject to the following conditions:

(a) Fresh proofs of identity and address shall not be sought at the time of periodic updation, from customers who are categorised as 'low risk', when there is no change in status with respect to their identities and addresses and a self-certification to that effect is obtained through customer's registered email-id, customer's registered mobile number, digital channels (such as online customer portal, mobile application, whatsapp customer service number), letter/post etc.
(b) A certified copy of the proof of address forwarded by 'low risk' customers through registered email-id, customer's registered mobile number, digital channels (such as online customer portal, mobile application, whatsapp customer service number), letter/post etc. in case of change of address shall be acceptable. The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
(c) Physical presence of low risk customer at the time of periodic updation shall not be insisted upon unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through registered email-id, customer's registered mobile number, digital channels (such as online customer portal, mobile application, whatsapp customer service number), letter/post etc., shall be acceptable.
(d) Company may obtain a copy of OVD or deemed OVD, or the equivalent e-documents thereof, as defined above, for the purpose of proof of address, declared by the customer at the time of periodic updationAcknowledgment with date of having performed KYC updation will be provided.
(e) Livephotographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

Additional measures: In addition to the above, 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, company may consider making available the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated. 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.

Commented [SV3]: Check what policy should be constructed

14) **Obtaining Permanent Account Number (PAN)**

The Company shall obtain and verify the Permanent Account Number or equivalent e-document thereof while undertaking transactions as per the provisions of Income Tax Rule 114B, as amended from time to time.

Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

Company shall to it by such date as may be notified by the Central Government, failing which company shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided further that if a customer having an existing account-based relationship with the company gives in writing to the company that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer i.e. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

Enhanced Due Diligence

Following EDD measures shall be undertaken by Company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

a) V-CIP shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

c) In case of request of change in registered mobile number, firstly, will not be encouraged but if required the new number requested must also be linked to Aadhaar. In case of additional contact number same will be available but for all account related purposed old number will be used.

d) Apart from obtaining the current address proof, company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

e) Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

f) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

g) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

Commented [SV4]: Important, if EDD is done then does this mean customer must be categorised as high risk

Commented [SV5R4]: To be checked as little tricky. Check for market practices

Secrecy Obligations and Sharing of Information:

(a) 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, company 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 Company requires disclosure and

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

Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to a company, with an explicit consent to download records from CKYCR, then such comanpy 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 –
(i) there is a change in the information of the customer as existing in the records of CKYCR;
(ii) the current address of the customer is required to be verified;
(iii) the company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
(iv)the validity period of documents downloaded from CKYCR has lapsed.

15) Money Laundering and Terrorist Financing Risk Assessment[i]

i) The Company will 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 will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company will take cognizance of the overall sector-specific vulnerabilities, if any, that the RBI or FIU-India may share with the Company from time to time.

ii) The risk assessment by the Company will 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 will be determined by the Board, subject to minimum of annual review, in alignment with the outcome of the risk assessment exercise.

iii) The outcome of the exercise will be put up to the Risk Management Committee and will be available to competent authorities and self-regulating bodies.

iv) The Company will apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and will frame Board approved policies, controls and procedures in this regard. The Company will also monitor the implementation of the controls and enhance them, if necessary.

Customer Identification Procedure

Annexure I - Customer Identification Procedure Features to be verified and documents that may be obtained from customers

Customer Type	Documents
Individuals Legal name and any other names used – Correct permanent address	"Officially valid document" means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that, a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. b. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:- i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. property or Municipal tax receipt; iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

	d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. 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
Companies - Name of the company - Principal place of business - Mailing address of the company - Telephone /Fax Number	Certificate of incorporation; Memorandum and Articles of Association; Permanent Account Number of the company (from May 29, 2019) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and Officially valid documents for CDD in respect of Beneficial Owners, managers, officers or employees holding an attorney to transact on its behalf. the names of the relevant persons holding senior management position; the registered office and the principal place of its business, if it is different.
Partnership firms Legal name – Address Names of all partners and their addresses – Telephone numbers of the firm and partners	Registration certificate; Partnership deed; Permanent Account Number of the partnership firm and Officially valid documents in respect of Beneficial Owners, managers, officers or employees holding an attorney to transact on its behalf. the names of all the partners address of the registered office, and the principal place of its business, if it is different

Commented [KM6]: This may be streamlined with requirements prescribed above

Trusts & foundations - Names of trustees, settlers, beneficiaries and Signatories Names and addresses of the founder, the managers / directors and the Beneficiaries - Telephone / fax numbers	Registration certificate: Trust deed; Permanent Account Number or Form No.60 of the trust and Officially valid documents in respect of Beneficial Owners, trustees / managers / the person(s) holding a power of attorney to transact on its behalf. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust the address of the registered office of the trust; and
Accounts of Unincorporated association or body of individuals	Resolution of the managing body of such association or body of individuals; Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals (from May 29, 2019) Power of attorney granted to him to transact on its behalf; An officially valid document in respect of the person holding an attorney to transact on its behalf; and such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.

Interpretation of KYC guidelines

Except what is stated in this policy, no interpretation of guidelines should be made. For any clarification, a reference must be made to the concerned official responsible for the compliance of Know Your Customer and Anti-Money Laundering norms with the Company.

The detailed guidelines of the Know Your Customer norms for individual borrowers and guarantors forming party to the Education Loan have been elaborated below:

Officially valid document containing details of his identity and address
PRE-REQUSITES

- Must be issued by appropriate authority
- Must necessarily have a live photograph of the concerned person duly attested by signing and stamping across the live photograph, wherever applicable
- Must be a valid document – not crossed its date of expiry

In addition to one live photographs of each of the borrowers, any one of the following documents would only be accepted by the Company.Passport

A valid / unexpired Passport issued by Government of India mentioning the name, address, photograph and validity in terms of expiry date. A valid passport is the one which is not expired and within the expiry date mentioned on the passport. The name, address and live photograph mentioned in the application form by the borrower must match with the name, address and photograph mentioned on the valid passport.

Driving License

A valid Driving License issued by Regional Transport Office (RTO) which has not expired and which is within the expiry date mentioned on the driving license. A valid driving license mentions the name and bears a photograph pasted with RTO stamp put across on it and signed by the RTO officer as applicable. The name and live photograph in the application form of the borrower must match with the name and photograph on the valid driving license.

Proof of possession of Aadhaar number

The use of Aadhaar, proof of possession of Aadhaar, eAadhaar, mAadhaar, etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Voters ID

Voters ID issued by Election Commission of India mentions name, photograph and address of the holder. However, the Voters ID would be accepted as valid Photo ID by the Company if the name and photograph matches with that on the application form. Voters ID is not accepted as address proof.

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

Letter issued by the National Population Register containing details of name and address.

Date of Birth Proof of the Borrowers

Following documents would only be accepted as date of birth proofs by the Company provided the name and other information matches with the information provided in the application form by the Borrowers.

PAN Card
Passport
Birth Certificate
SSC Passing Certificates (wherever date of birth is mentioned)
School or College Leaving Certificate
Photo ID issued by State or Central Government of India (wherever date of birth is mentioned)
Driving License being issued by the RTO

Central KYC Records Registry

The Central Government in consultation with the Reserve Bank of India has notified Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015 from July 7, 2015 for formation of the Central KYC Records Registry. Further vide notification dated November 26, 2015 the Central Government has notified Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), set up under sub-section (1) of Section 20 of the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 to act as the Central KYC Records Registry. The RBI has vide its Circular dated December 8, 2016 made changes to its Master Direction - Know Your Customer (KYC) Direction, 2016 instructing all Regulated Entities other than Scheduled Commercial Banks to upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR.

In accordance with the above changes, the Company will follow the below rules

The Company shall within ten days after the commencement of an account- based relationship with a client, file the electronic copy of the client's KYC records with the Central KYC Records Registry.

The Central KYC Records Registry shall issue a KYC Identifier for each client to the Company, which shall be communicated to the client in accordance with the Company's procedure.Where a client, for KYC purpose, submits a KYC Identifier to the Company, then the Company shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless –

there is a change in the information of the client as existing in the records of Central KYC Records Registry;the current address of the client is required to be verified;the Company considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

The Company after obtaining additional or updated information from a client under sub rule (1C), shall within seven days or within such period as may be notified by Central Government, furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client.

The Company shall make necessary changes in its procedures to comply with the above requirements.

The Company shall comply with the changes in the laws, rules, directions and guidelines issued by the Reserve Bank of India and applicable to the Company from time to time and the rules shall override this policy of theCompany.

Digital KYC Process

A. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of the 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 the Company) 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/e-Aadhaar 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 form 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.

Annexure II – Risk Categorization of Customer Profile

The Company shall monitor all its transactions from money laundering risk perspective, which may be unique to its products, services, distribution channels, administration and local jurisdiction, with specific attention to complex and unusually large transactions which have no apparent economic or visible lawful purpose. The Company shall periodically review profile of new and/ or existing customers against lists of prohibited individuals and entities issued by the United Nations or any other regulatory /statutory authorities. Such due diligence must be conducted based on the risk categorization of customers, inter alia detailed as under.

Low Risk – These customers can be those whose identity and source of wealth can be easily identified and those who have undergone the prescribed KYC process.

Medium Risk – These customers will typically include inter-alia (a) Non-Resident Customers (b) High Net Worth Individuals categorized on the basis of the customer's back ground, nature and location of activity, country of origin, sources of funds and customer profile.

High Risk – These customers will typically include inter-alia (a) firms with silent partners, (b) politically exposed persons of foreign origin, (c) person with doubtful reputation as per public information available (d) customer based in a high-risk country (e) customer working for a company based in a high-risk country or (f) customer on deputation to a high-risk country by his employer based in a regulated country

The said 'high risk customer' must be subjected to additional diligence and their transactions may be supervised/monitored.

The Company must ensure that diligence initiated in respect of its customers under the KYC norms is kept strictly confidential and no tip-off is given to the concerned customer and/ or his agent.

Moreover in case of Politically Exposed Person (PEP), the decision to undertake any transaction with such person(s) should be taken by the COO and no account shall be opened in fictitious/benami name(s)/entity(ies).

Required Compliance

The following compliance is required to be done based on the above-mentioned Risk Categorization

Low Risk	Full KYC exercise once every 10 years
Medium Risk	Full KYC exercise once every 8 years
High Risk	Full KYC exercise once every 2 years

Reporting to FIU-IND

Cash Transaction	**Time period within which to be reported**	**Form**
Cash Transaction of the value in excess of Rs. 10 lacs or its equivalent in foreign currency during one calendar month	Within the 15th day of the succeeding calendar month.	CTR
All series of cash Transaction integrally connected to each other which have been valued below Rs. 10 lacs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value exceeds Rs. 10 lacs	Within the 15th day of the succeeding calendar month.	CTR
Suspicious Transaction	**Time period within which to be reported**	**Form**
All suspicious transactions whether or not made in cash and by way of as	Not later than 7 working days on	STR

mentioned in Rule 3 D (i)-(v) of the PML Rules and including cases where the branch have reasonable ground to believe that the transaction involve proceeds of crime. [1] Further even attempted transactions should be reported, even if not completed by the customers. Irrespective of the amount of the transaction.[1]	being satisfied that the transaction is suspicious	
Forged or Counterfeit Currency Transaction	**Time period within which to be reported**	**Form**
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 transaction.	Not later than 7 working days from the date of occurrence of such transaction	STR

The Company is committed to adhering to international obligations under the UAPA Act, 1967, and the WMD Act, 2005 as advised. The Company shall diligently verify customer identities against the United Nations Security Council sanctions lists and ensure compliance with all relevant guidelines, including enhanced due diligence for jurisdictions that insufficiently apply FATF recommendations. The Company shall maintain rigorous processes to monitor and report any transactions related to designated individuals or entities, ensuring a robust approach to mitigating risks associated with terrorism financing and the proliferation of weapons of mass destruction.

References

Pursuant to the guidelines provided under Circular DBR.AML.BC.No.81/14.01.001/2015-16 dated Nov 6, 2024