Policy on Know Your Customer and Anti-Money Laundering Measures
Table of Contents

Sr. No	Contents	Pg. No.
1	Introduction	2
2	Objective	2
3	Customer Acceptance Policy (CAP)	2
4	Customer Identification Procedure (CIP)	3
5	Required KYC due diligence for all customers	5
6	Identification	5
7	Verification	6
8	Resolution of discrepancies	9
9	Reporting	9
10	Records retention	10
11	Customer CIP notice	11
12	Existing customers	11
13	Enhanced due diligence	11
14	Reliance on third party due diligence	12
15	Periodic updation of KYC	13
16	Risk categorization	14
17	Monitoring of Transactions	15
18	Risk Management	15
19	Employee Training	15
20	Applicability to branches and subsidiaries outside India	16
21	Introduction of new technologies	16
22	Appointment of Designated Director / Principal Officer	16
23	Review of Policy	16
Annexure – I	Risk Categorisation	17
Annexure – II	Customer Identification Requirements	18
Annexure – III	Customer Identification Procedure	21
Annexure – IV	Suspicious transactions	25

Policy on Know Your Customer and Anti- Money Laundering measures

1) Introduction:

Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-money Laundering (AML) standards and has advised all regulated entities including NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company across all its branches in India.

2) Objective:

Objective of RBI guidelines is to prevent the regulated entities from being used, by criminal elements as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. The guidelines also mandate making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

This policy seeks to provide guidance to the businesses to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. The Company shall adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

3) Customer Acceptance Policy:

The Company shall follow the following norms while accepting and dealing with its customers:

- No account is opened in any anonymous or fictitious / benami name.
- Carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the applicant is not known or the Company is unable to apply appropriate CDD measures, no transaction or account-based relationship will be undertaken with such person / entity.

- A Unique Customer Identification Code (UCIC) shall be allotted by the Company while entering into new relationships with individual customers. The Company shall apply CDD measures at the UCIC level.
- Parameters of risk perception are clearly defined in terms of customer identity, nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions etc. to enable categorization of customers into low, medium and high risk. The illustrative list of such risk categorisation is provided in annexure – I.
- The customer profile contains mandatory information to be sought for KYC purpose relating to customer's identity, address, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risks perceived by the Company. However, while preparing customer profile the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross selling or any other purpose. The Company shall maintain secrecy regarding customer information except where the disclosure is under compulsion of law, there is a duty to the public to disclose, the disclosure is made with express or implied consent of the customer.
- The Company shall ensure that the identity of the customer does not match with any person or entity whose name appears in the sanction lists / designated lists circulated by RBI from time to time.
- The intent of the Policy is not to result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged including persons with disabilities. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers and no application shall be rejected without application of mind. Reason for rejection shall be duly recorded by the Company.
- When the true identity of the account holder is not known or where the company forms a suspicion of money laundering or terrorist financing and it reasonably believes that performing the CDD process will tip-off the customer the Company shall file Suspicious Transaction Reporting (STR) as provided below in clause 9 and shall not pursue CDD process.

4) Customer Identification Procedure:

The Company shall undertake identification of customers before commencement of an account-based relationship. Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious/ anonymous/ benami person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

An effective Customer Identification Program ("CIP") is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

- verify the identity of any Person transacting with the Company to the extent reasonable and practicable;
- maintain records of the information used to verify a customer's identity, including name, address and other identifying information and

- verify the United Nations Security Council (UNSC) sanctions lists under Unlawful Activities (Prevention) (UAPA) Act, 1967 / designated list under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 / UNSCR 1718 Sanctions List of Designated Individuals and Entities / FATF statements of known or suspected terrorists or terrorist organizations / jurisdictions and countries that do not or insufficiently apply the FATF recommendations as provided to the Company by RBI or any other applicable government agency to determine whether a person opening an account or an existing customer appears on any such list. The Company shall verify the above sanction lists on a daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company.

- apply enhanced due diligence, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

The Company will carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise quarterly basis to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc. The internal risk assessment carried out by the Company should commensurate to its size, geographical presence, complexity of activities/structure, etc. and shall apply a Risk Based Approach and implement a CDD programme, having regard to the ML/TF risks identified for mitigation and management of the identified risks. Respective businesses shall have standard operating procedures for identification, mitigation, controls and procedures for management of the identified risk, if any. The risk assessment processes shall be reviewed periodically to ensure its robustness and effectiveness.

5) Required KYC Due Diligence for all customers:

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements.

6) Identification:

All the customers shall be identified by a unique identification code to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

The customer identification requirement is detailed in annexure II to this policy. Each business process shall implement procedures to obtain from each Customer (including non-face-to-face customers), prior to transacting, the following information as may be relevant, to that business:

a) Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the loan;
b) For individuals - age / date of birth; For a person other than individual (such as corporation, partnership or trust) - date of incorporation;
c) Complete address of the customer including the documentary proof thereof;
    i. For an individual, a residential or business street address;
    ii. For a Person other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;
d) Telephone/Fax number/E-mail ID;
e) Identification number:

    i) A taxpayer identification number; passport number and country of issuance; proof of possession of Aadhaar number; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard or the unique number or code assigned by the Central KYC Records Registry. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government-issued documentation certifying the existence of the business or enterprise;

    Where a customer submits proof of possession of Aadhaar number, the Company shall ensure that such customer redacts or blackout his Aadhaar number before submitting the same to the Company.

ii) For a customer who has applied for, but has not received an identification number, loan may be sanctioned, but each business process shall implement procedures to confirm that the application was filed before the loan is sanctioned to customer and to obtain the identification number within a reasonable period of time before disbursal of loan.

f) One recent photograph of the individual customer. Fresh photographs will be obtained from minor customer on becoming major.

For undertaking CDD, the list of documents that can be accepted as proof of identity and address from various customers across various products offered by the Company is given as **annexure III** to this policy. These are appropriately covered in the credit policies of the respective businesses and communicated to the credit approving authorities.

7) Verification:

Each business process as a part of the credit policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

i. Verification through documents:

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in annexure - III to this policy. These are appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

ii. Verification through non-documentary methods: These methods may include, but are not limited to:

1. Contacting or visiting a customer;
2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
3. Checking references with other financial institutions; or

4. Obtaining a financial statement.

iii. Aadhaar based e-KYC authentication / face authentication:

Where the customer submits Aadhaar number, the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility or Aadhaar face 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 and the company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

However, the Aadhaar-based face authentication shall not result in exclusion of customers with disabilities or special needs. In cases where a customer is unable to successfully complete Aadhaar based face authentication (including situations such as disfigurement or medical conditions), suitable alternate KYC methods shall be permitted.

iv. *Offline verification through proof of possession of Aadhaar number:*

The Company may carry out offline verification of a customer under the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (Aadhaar Regulations) if the customer is desirous of undergoing Aadhaar offline verification for identification purpose.

No such offline verification will be performed without obtaining the written consent of the customer in the manner prescribed in the Aadhaar Regulations.

The Company shall not collect, use or store an Aadhaar number of its customer for any purpose.

v. Aadhaar OTP based e-KYC:

The Company may carry out Aadhaar OTP based e-KYC in non-face-to-face mode with a specific consent from the customer for authentication through OTP. The transaction alerts, OTP, etc., shall be sent only to the mobile number of the customer registered with Aadhaar. For such borrowal account, the aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year. Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless detailed customer due diligence is carried out.

vi. Verification of equivalent e-document:

Where the customer submits an equivalent e-document of any Officially Valid Document (OVD), issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer, the Company

shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take live photo of the customer as specified under digital KYC in RBI regulations.

vii. Verification through digital KYC:

The Company may carry out verification by capturing live photo of the customer and OVD or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with latitude and longitude of the location where such live photo is being taken by the authorized officer of the Company as prescribed in RBI regulations.

The Digital KYC process shall be performed through a secure, authenticated application. Access to this application shall be strictly controlled by the Company, ensuring that only Authorised Officials and designated third-party agents ("Agents") are permitted to perform the Digital KYC process. Authorised Officials/Agents shall access the application only through a login-id and password or a Live OTP or Time OTP controlled mechanism provided by the Company.

viii. Video based customer identification process (V-CIP):

The Company may undertake live V-CIP for establishment of an account-based relationship with an individual customer after obtaining his informed consent and adhering to the procedures / minimum standards prescribed in RBI regulations. The official carrying out V-CIP shall be capable of testing liveliness check to detect any fraudulent manipulation or suspicious conduct. However, such liveliness check shall not result in exclusion of person with disabilities. This process shall be treated as face-to-face process for the purpose of customer identification.

ix. *Change of Registered Mobile Number for Non-Face-to-Face Accounts*

The Company shall establish a process for handling requests for change of registered mobile number in accounts opened through non-face-to-face modes. Any such modification shall be executed only after due verification of the customer's identity, followed by validation of the new mobile number.

x. Retrieval of KYC records from CKYCR:

Where a customer submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, the Company may 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 unless–

- there is a change in the information of the customer as existing in the records of CKYCR;
- the current address of the customer is required to be verified;

- 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;

- the validity period of documents downloaded from CKYCR has lapsed.

- the record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the regulators.

If an update in the KYC record of an existing client is informed by the Central KYCR, the company shall retrieve the updated KYC records from the Central KYCR and update the KYC record maintained by the company as per the guidelines issued by the regulators.

The Company while downloading and relying on KYC records from the CKCYR shall not be required to re-verify the authenticity of customer's identity and / or address, provided the KYC records downloaded are current and compliant with the PML Act, 2002 / PML Rules, 2005.

8) Resolution of Discrepancies:

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

9) Reporting:

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and cash transactions greater than Rs. 10 lakhs, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or bona fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

e) Where the transactions are abandoned by customers on being asked to give some details or to provide documents

Illustrative list of activities which would be construed as suspicious transactions are given in Annexure IV to this policy.

Further, the Principal officer shall furnish information of the above-mentioned transactions to the Director, Financial Intelligence Unit – India (FIU-IND) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the Principal officer, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued greater than Rs.2 lakhs so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

The Company shall not put any restriction on operations in the accounts where a suspicious transaction report (STR) has been filed. The Company shall keep the fact of furnishing of STR strictly confidential and shall ensure that there is no tipping off to the customer at any level.

The Company shall upload the KYC information pertaining to individuals / legal entities, as applicable from time to time, with Central KYC Records Registry (CKYCR) in terms of provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

10) Records Retention:

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures including updated records of the identification data of customer and their beneficial owners, account files, business correspondence and results of any analysis undertaken. The business process shall implement, at a minimum, the following procedures for retaining records:

a. Transactions for which records need to be maintained:

i. All cash transactions of the value of more than Rs. 10 lakhs.
ii. All series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lakhs where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs. 10 lakhs.
iii. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place.
iv. All suspicious transactions whether or not made in cash.

b. Information to be preserved:

The information required to be preserved with respect to the above transactions are the nature of transactions, amount, date of transaction and the parties to the transaction.

c. Periodicity of retention:

The following records shall be retained for a minimum period of five years after the business relationship is ended:

i. The customer identification information (including information of beneficial owners) and residence identification information including the documentary evidence thereof.

ii. All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity.

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained for a period of at least Ten (10) years after such record was created.

The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request.

11) Customer CIP Notice:

Each business process shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to account opening.

12) Existing Customers:

The requirements of the earlier sections are not applicable to accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the KYC document available with the Company are the updated documents / information as confirmed by the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the due diligence measures.

13) Enhanced Due Diligence:

The Company is primarily engaged in retail finance. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. The Company shall also undertake enhanced due diligence in case of non-face-to-face onboarding facilities (such as CKYCR, DigiLocker, equivalent e-document, etc.) for establishing the relationship with the customer without meeting the customer physically or

through V-CIP. 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.

Each business process in its credit policy shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence.

Enhanced Due Diligence shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

(i) Customers requesting for frequent change of address/contact details
(ii) Sudden significant change in the loan account activity of the customers
(iii) Frequent closure and opening of loan accounts by the customers

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

14) Reliance on third party due diligence:

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the Company may rely on a third party; subject to the conditions that-

a) the Company obtains records or information of such customer due diligence carried out by the third party immediately from the third party or from 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.

15) Updation / Periodic updation of KYC:

The Company shall have a system of risk-based approach in place for periodical updation of customer identification data after the account is opened ensuring that the information or data collected is kept up-to date and relevant particularly when there is a high risk. KYC updation will be carried out at a periodicity not less than once in ten years in case of low-risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers from the date of opening of the account / last KYC updation.

To facilitate ease of access and customer convenience, the Company shall provide the facility to undertake KYC updation and periodic updation of KYC of its customers through any of its branches or such other available channels.

Customers need not submit fresh KYC documents at the time of periodic updation, in case of no change in status with respect to their KYC information and a self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such customers, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, digital channels, letter etc., and the declared address shall be verified through positive confirmation within two months by means of address verification letter, contact point verification, deliverables etc. The Company may at its discretion, obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.

Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation of KYC, as per the procedure prescribed in RBI Regulations.

For customers other than Individual, the Company shall ensure that during the above process, Beneficial Ownership (BO) information available with it is accurate and shall update the same, if required, to keep it as up-to-date as possible. In case of change in KYC information of customers other than individual, the Company shall undertake the KYC process equivalent to that applicable for on-boarding a new non-individual customer.

In case any existing customer fails to submit PAN or equivalent e-document or Form No.60, the Company shall temporarily cease operations in the account till the time the same is submitted by the customer. For the purpose of ceasing the operation in the account, only credits shall be allowed.

However, for customers who are unable to provide PAN or equivalent e-document or Form No.60 owing to injury, illness or infirmity on account of old age or such like causes, the Company will continue operation of accounts for such customers subject to enhanced monitoring of the accounts.

In case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship, the customers shall

submit the updated documents to the Company within 30 days of the update, for the purpose of updating the records at Company's end.

The Company shall intimate customers in advance prior to the due date of periodic updation to update their KYC. The intimations shall be sent well in advance with at least three advance intimations including at least one intimation by letter at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Further, subsequent to the due dates, the Company shall also send at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimation. The Company shall also communicate to the customer the consequence of failure to update their KYC in time through such intimations / reminders. Such communications sent to customers shall be duly recorded in the system for audit trail.

Such periodic updated information / documents submitted by the customers shall be promptly updated in the records / database of the Company and an intimation mentioning the date and status of updation of KYC details shall be provided to the customer.

16) Risk Categorisation:

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of businesses is provided in Annexure - I. Each business process adopts the risk categorization in their respective credit policies based on the credit appraisal, customer's background, nature and location of business activity, country of origin, sources of funds, client profile, etc. and all parameters of risk perception as defined in the customer acceptance policy above. Where businesses believe that a particular customer falling under a category is in his judgement falling in a different category, he may categorise the customer so, so long as appropriate justification is provided in the customer file.

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

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

17) Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has 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 of the account. The different business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible legitimate purpose. High-risk accounts have to be subjected to intensified monitoring.

The Company shall put in place an appropriate software application / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. The Company may consider adopting appropriate innovations including artificial intelligence and machine learning technologies to support effective monitoring.

18) Risk Management:

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

Company's internal audit and compliance functions play a role in evaluating and ensuring adherence to the KYC policies and procedures.

As a general rule, the compliance function also provides an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements.

Internal Auditors specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance in this regard is put up before the Audit Committee of the Board on quarterly intervals. The Company ensures that the decision-making functions of determining compliance with KYC norms are not outsourced.

19) Employee Training:

The Company on an ongoing basis educates the front-line staff, the branch staff and the new joinees on the elements of AML / KYC / CFT through various training programmes, training e-modules and e-mails. The Company shall ensure that, the staff dealing with KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape. The management on an ongoing basis shall ensure an environment which fosters open communication and high integrity amongst the staff.

20) Applicability to branches and subsidiaries outside India:

The Company does not have operations/subsidiaries outside India.

21) Introduction of new technologies:

Respective business unit in co-ordination with the Risk management division shall identify and assess the money laundering (MF) / terrorist finance (TF) risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products and shall ensure to undertake the ML/TF risk assessments prior to the launch or use of new products, practices, services, technologies; and to adopt a risk-based approach to manage and mitigate the risks through appropriate enhanced due diligence measures.

22) Designated Director / Principal Officer:

Mr. Ravindra Kumar Kundu, Managing Director will be the designated director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules. Ms. P Sujatha is designated as Principal Officer who shall be responsible for furnishing of information to FIU-IND.

'Senior Management' for the purpose of compliance and implementation of KYC policy shall be Mr. Ravindra Kumar Kundu, Designated Director and Ms. P Sujatha, Principal officer.

23) Review of Policy:

This policy is subject to review from time to time and such changes as are required based on regulatory changes may be approved by the Managing Director.

*****

Annexure – I

Indicative list for Risk Categorisation

Low Risk Category

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk.

Illustrative examples are:

- Salaried employee
- Self-employed individuals / Proprietary firms Government departments and Government-owned companies
- Public Limited and Private Limited Companies
- Partnership Firms with registered partnership deed
- Statutory bodies & Regulators
- Hindu Undivided Family (HUF)

Medium & High-Risk Category

Customers that are likely to pose a higher-than-average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples of medium risk category customers are:

a) Non-Resident customers
b) Trust, Charities, NGO's and Organization receiving donations
c) Firms with majority 'sleeping partners' (more than 51%)

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs)
2. Bullion dealers and dealers of precious stones/ metals
3. All non-face to face customers

Annexure - II

Customer Identification Requirements

Trust/Nominee or Fiduciary Accounts

In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. Company takes reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Accounts of companies and firms

Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who comprise the management.

These requirements may be moderated according to the risk perception e.g. in the case of a public company.

Client accounts opened by professional intermediaries

Where the transaction is with a professional intermediary who in turn is on behalf of a single client, that client must be identified. The Company shall not open accounts with such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, including the Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials.

The Company offers products primarily to Indian residents only. The Company if extending any finance to non-residents should check if he is PEP and check all the information available about the person in the public domain. Further, apart from performing normal due diligence, the company shall take reasonable measures to establish the source of funds/wealth. The decision to transact with the PEP should be

taken only by the Head of credit of the respective businesses supported by appropriate verification. The Company is also required to subject such accounts to enhanced monitoring on an ongoing basis. The above norms shall also be applied to the contracts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the approval of the Head of respective businesses shall be obtained to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Identity of Beneficial Owner

The Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a customer and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership

(a) 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 person, has a controlling ownership interest or who exercises control through other means.

Explanation:

I. "Controlling ownership interest" means ownership of or entitlement to more than ten percent of shares or capital or profits of the company;

II. "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;

(b) 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 ownership of/entitlement to more than ten percent of capital or profits of the partnership;

(c) where the customer 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;

(d) 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;

(e) where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten 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. In case the customer is acting on behalf of another person as trustee / nominee, the Company shall obtain satisfactory evidence of the identity of the persons on whose behalf they are acting; and

(f) where the customer or the owner of the controlling interest is an entity listed on a stock exchange in India, or is a subsidiary of such a listed entity, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Non-Profit Organisations:

Non-profit organisations are those entities or organisations, which are constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961, and which are registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

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

Annexure III

Customer Identification Procedure – KYC documents that may be obtained from customers

Nature of customer	List of applicable documents
Individual	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: a) Aadhaar number where the individual decides to submit his Aadhaar number voluntarily to the Company notified under first proviso to sub-section (1) of section 11A of the PML Act; b) proof of possession of Aadhaar number where offline verification can be carried out; or c) a certified copy of any OVD containing details of his identity and address or the equivalent e-document thereof; or d) the KYC Identifier with an explicit consent to download records from CKYCR; e) the Permanent Account Number (PAN) or Form no.60; and f) such other documents as specified by the Company from time to time. **List of OVDs**: i) Passport ii) Driving license iii) Proof of possession of Aadhaar number iv) Voter's identity card issued by the Election Commission of India v) Job card issued by NREGA duly signed by an officer of the State Govt. vi) Letter issued by the National Population Register containing details of name and address. **Provided that**: 1) 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 UIDAI. 2) 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 Govt. or Central Govt. 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; 3) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at '(2)' above 4) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. **Explanation**: 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.
Hindu Undivided Family (HUF)	1) PAN in the name of HUF; 2) Certified copy of any OVD containing details of identity and address of KARTA / authorised signatories of the HUF or the equivalent e-document thereof; 3) HUF Letter/ Declaration signed by all the coparcener and KARTA; 4) Copy of HUF deed.
Sole Proprietary firms	1) Customer due diligence of the individual proprietor shall be carried out as applicable / specified for Individual. 2) In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained: a) Registration certificate including Udyam Registration certificate issued by the Government. b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. c) Sales and income tax returns. d) CST/VAT/ GST certificate (provisional/final). e) Certificate/registration document issued by Sales Tax/Service

	Tax/Professional Tax authorities. f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. h) Utility bills such as electricity, water, landline telephone bills, etc. **Explanation**: In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business/activity after recording the appropriate reason for accepting one document. The Company shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
Company	Certified copies of each of the following documents shall be obtained: a) Certificate of incorporation b) Memorandum and Articles of Association c) Permanent Account Number of the company d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf e) Documents, as specified for Individual, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf f) Names of the relevant persons holding senior management position (For the purpose of this section, senior management means managing director, chief executive officer, manager, whole-time director, company secretary and chief financial officer) g) Address of the registered office and the principal place of business, if it is different.
Partnership Firm	Certified copies of each of the following documents shall be obtained: a) Registration certificate b) Partnership deed c) Permanent Account Number of the partnership firm d) Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf e) The names of all partners f) Address of the registered office and the principal place of business, if it is different.
Trust	Certified copies of each of the following documents shall be obtained:

	a) Registration certificate b) Trust deed c) Permanent Account Number or Form No.60 of the trust d) Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf e) Names of the beneficiaries, trustees, settlor and protector if any and authors of the trust; f) Address of the registered office of the trust g) List of trustees and KYC documents for those discharging the role as trustee and authorised to transact on behalf of the trust.
Unincorporated Association or a Body of Individuals	Certified copies of each of the following documents shall be obtained: a) Resolution of the managing body of such association or body of individuals b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals c) Power of attorney granted to transact on its behalf d) Documents, as specified for Individual, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and e) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals. **Explanation**: (i) Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'. (ii) Term 'body of individuals' includes societies.
Juridical persons not specifically covered above, such as societies, universities and local bodies like village panchayats etc. or who purports to act on behalf of such juridical person or individual or trust	Certified copies of the following documents shall be obtained: a) Document showing name of the person authorised to act on behalf of the entity; b) Documents, as specified for Individual, of the person holding an attorney to transact on its behalf and c) Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Note: *Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notified by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.*

Annexure - IV

Illustrative list of activities which would be construed as suspicious transactions

- Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.
- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
  - A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
  - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.
  - An account where there are several cash transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.
- Certain Employees of the Company arousing suspicion:
  - An employee whose lavish lifestyle cannot be supported by his or her salary.
  - Negligence of employees/willful blindness is reported repeatedly.
- Some examples of suspicious activities/transactions to be monitored by the operating staff:
  - Multiple accounts under the same name
  - Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc,
  - There are reasonable doubts over the real beneficiary of the loan
  - Frequent requests for change of address