Know Your Customer and Anti Money Laundering Policy

BOD meeting dated 30 January 2026
Resolution no. ---

Know Your Customer and Anti Money Laundering Policy

I. Introduction:-

Reserve Bank of India had issued various guidelines to primary (Urban) Co-operative Banks, since 2002 onwards in regard to "Know Your Customer" and has advised the banks to prepare a policy of the Bank covering the K.Y.C. guidelines and subsequently directions Reserve Bank of India (Urban Co-operative Banks – Know Your Customer) Directions, 2025.

The purpose of this Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy is to establish a robust framework for detecting, preventing, and reporting any suspicious activity that may be related to money laundering, terrorist financing, or other financial crimes.

The KYC process involves verifying the identity of the customer, understanding the nature of their transaction, and assessing the risk associated with it. It is a fundamental part of customer due diligence and forms the first line of defense in preventing financial crime.

The AML framework includes internal controls, transaction monitoring, employee training, and reporting mechanisms to detect and respond to suspicious activities in a timely and effective manner.

II. Objectives:-

The KYC policy has been framed to develop a strong mechanism for achieving the following objectives

- To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.

- To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms/AML standards/ CFT measures/ Bank's obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.
-To put in place a proper control mechanism for detecting and reporting of suspicious transactions in accordance with the statutory and regulators provisions.
- To ensure that all the provisions of Prevention of Money Laundering Act, 2002 and the Rules made there under and all subsequent amendments thereto are duly complied with, and
- TO ensure compliance with guidelines/instructions issued by the regulators, including FIU-IND and RBI

III. Scope of the Policy:-

This policy is applicable to all branches and head office of the Bank for maintance of the customer ID and Customer data.

IV. Definitions

Person:- "Person" has the same meaning assigned in the Act and includes

An individual,
A Hindu undivided family,
A company,
A firm,
An association of persons or a body of individuals, whether incorporated or not
Every artificial juridical person, not falling within any one of the above persons and
Any agency, office or branch owned or controlled by any one of the above persons.

Customer:-

For the purpose of K.Y.C Policy, a customer is defined as:

- A person or entity that maintains an account and / or has a business relationship with Bank..
- And includes a person on whose behalf the person who is engaged in the transaction or activity, is acting,
- Walk in customer means a person who does not have an account based relationship with the bank, but undertake transactions with the bank.

Existing Customer :-

- An **existing customer** is a person or entity who has already established a business relationship with the bank

Individual Customer :-

- An **Individual Customer** is a **natural person** who establishes a relationship with the bank in their personal capacity. This includes customers who open or maintain accounts, conduct financial transactions, or avail services for personal use.

- E.g. Individuals opening saving or current accounts etc.

Non-Individual Customer :-

- A **Non-Individual Customer** refers to any **legal entity or artificial person**, other than a natural person, that establishes a business relationship with bank.

- These entities operate through authorized representatives and may include identification of ownership and control, including **beneficial owners**, as part of Customer Due Diligence (CDD) under KYC/AML regulations.

- E.g. Partnership Firms, Trusts, Societies, Private and Public Limited Companies etc.

Minor Customer

- A **Minor Account** is an account opened and maintained for a **natural person who is below the legal age of majority** (typically under 18 years).These accounts are operated by a **guardian or parent** on behalf of the minor until they reach the age of majority.

Beneficial Owner: -

- A **Beneficial Owner** is the **natural person(s)** who ultimately owns, controls, or has a significant influence over a customer (legal entity or arrangement) and/or the person on whose behalf a transaction is being conducted.
- Identifying the beneficial owner is a key requirement under KYC/AML regulations to ensure transparency and prevent the misuse of entities for money laundering or terrorist financing.

PEP (Politically Exposed Persons):-

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

KYC – Know Your Customer: -

- Know Your Customer (KYC) is a mandatory process under **Anti-Money Laundering (AML)** regulations that involves **identifying and verifying the identity of customers** before establishing a financial relationship.

Applicability of KYC:

- A customer intended to start any(fund based or non fund based) banking relation with the bank
- **A walk in customer**
- **Any person transacting with the banking system**
- Periodic updation of KYC
- Opening of a new account of new or existing customer

Re-KYC:-

- **Re-KYC** (Re-Know Your Customer), also known as **Periodic KYC Update**, refers to the process of **updating and re-verifying the identity and address details of an existing customer** at regular intervals, as required by KYC/AML regulations.

Applicability of Re-KYC:

- As per the extent guidelines and directions issued by the Reserve Bank of India time to time on KYC and AML, bank needs to categorise its customer into 3 category i.e. High Risk, Medium Risk and Low Risk customers.
- On completion of a defined vintage of the customer in the bank as per its risk category bank has to obtained fresh KYC from the said customer and it is treated as ReKYC.
- Bank has to obtain fresh KYC from the customer as per below matrix
  For Low Risk Customer - 10 Years
  For Medium Risk Customer - 8 Years
  For High Risk Customer - 2 Years
  (from account opening date or last update date)

CKYC - Central Know Your Customer:-

- Central Know Your Customer (CKYC**)** is a centralized KYC repository system introduced by the Government of India and managed by CERSAI (Central Registry of Securitization Asset Reconstruction and Security Interest of India**)**.
- Under CKYC, a customer's KYC details are uploaded to a **central registry**, and a unique **14-digit CKYC Identifier** is assigned to the customer. This enables customers to complete KYC once and use the same CKYC number across multiple financial institutions, thereby avoiding duplication and enhancing compliance with **Anti-Money Laundering (AML)** norms.

NPO (Non-profit organizations):-

- "Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is 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 (18 of 2013).
- **Ex.** Charitable Trusts, Religious Institutions, NGOs etc.

DARPAN ID:

As per PMLA Rules-2005, it is mandatory for all Non-profit Organizations (NPOs) like Trusts, Societies and Section-8 Companies, who have established Trust/ Society/ Company for

Charity or Religious or Non-profit Making activities such as "Relief to the poor, education, medical relief, are required to mandatorily Register themselves in the DARPAN Portal of NITI Aayog and are required to submit DARPAN ID to the Bank.

In case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. Bank should preserve the record of DARPAN ID for a period of five years after the business relationship between the customer and the bank has ended or the account has been closed, whichever is later.

Simplified Due Diligence (SDD)

The Bank may apply Simplified Due Diligence (SDD) measures to customers who are assessed and categorised as low risk, based on the Bank's approved risk assessment framework, in accordance with the provisions of the Reserve Bank of India Know Your Customer (KYC) Directions, as amended from time to time.
While applying SDD, the Bank shall ensure full compliance with the minimum KYC requirements, including customer identification, verification of identity and address, and capture of such information and documents as prescribed under the applicable KYC Directions at the time of account opening and periodic updation.
The Bank shall not apply Simplified Due Diligence in cases where the customer or transaction is identified as high risk, or where there are suspicious transactions, adverse information, or doubts about the adequacy or authenticity of customer information.

Customer Due Diligence (CDD) –

To strengthen the process of Customer Identification and risk management bank should Exercise Customer Due Diligence whenever is required irrespective of the customer profile or risk category. Customer due diligence is a means of process to understand the customer profile and nature of transaction deeply. It will also enable the bank to establish correct relationship between beneficial owners with the account. Customer Due Diligence mention in Annexure VII.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable
b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification..

On Going Due Diligence: - Branches shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers,

customers' business and risk profile, the source of funds / wealth, and in regard to the Money Laundering and Terrorist Finance risks.

V. <u>Components of the Policy: -</u>

There are following four component / element of the "Know Your Customer" Policy.

a) Customer Acceptance Policy;
b) Risk Management;
c) Customer Identification Procedures (CIP); and
d) Monitoring of Transactions

a) <u>Customer Acceptance Policy (C.A.P):-</u>

In terms of RBI guidelines, the Customer Acceptance Policy (CAP) is one of the four parameters, which broadly define the KYC/AML/CFT guidelines. The CAP has been framed for ensuring compliance with all applicable regulatory guidelines while establishing customer relationship and maintaining the related accounts as per profile of the customers, the details are as under,

.

i. No account shall be opened in anonymous, fictitious, benami, shell companies.

ii. No accounts shall be opened where Bank is not able to apply Customer Due Diligence (CDD) measures either due to non-cooperation of the customer or non-reliability of the KYC documents / information furnished by the customer / applicant. The bank shall consider filling as STR, if necessary when it is unable to comply with the relevant CDD measures in relation to the customer. **Bank may exercise right to denial of services and restrict the customer from operations in the account, in case of any KYC non-compliance. Provided customer has to be intimated for atleast of 3 times through SMS or email (1 should be written notice) for the submission of compliance.**

iii. The mandatory information shall sought for KYC purpose at the time of opening an account and during periodic updating. Any optional/ additional information shall be obtain with the explicit consent of the customer after opening of the account.

iv. CDD procedure shall applied at the Unique Customer Identification Code (UCIC) level. Accordingly, no fresh CDD exercise shall be required while opening another account by any existing customer in the Bank.

v. CDD procedure shall follow for all individuals including all joint account holders while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder, related to any legal entity.

vi. "**Beneficial Owner"** shall be identify / verified necessarily while opening / maintaining accounts having constitution as Partnership, Limited Companies, Trust etc.

vii. **Name screening** of the prospective customer, before opening any account to be ensure that the identity of the prospective customer does not match with any person having known criminal background or with banned entities such as individual terrorists or terrorist organizations as advised by UN sanctions, GOI, FIU-IND and RBI list being published from time to time. These lists have been made available through AML/KYC software.
It should be ensured that this list should update regularly.

viii. Wherever accounts are opened and be operated by mandate holder or accounts are opened by intermediaries in fiduciary capacities, it should be ensured that the circumstances in which the said mandate holder or intermediary is permitted to act on behalf of another person/ entity are clearly spelt out, in conformity with the established law and practice of banking.

ix. If the customer is a **Politically Exposed Person (PEP)** as per knowledge of the Bank, the account of such person will be approved by Branch Head before opening.

x. Re-KYC exercise shall be carried out as per risk profile/ category of the customers and fresh set of KYC documents shall be obtained either digitally or physically. In case of any suspicious activities observed bank may insist the account holder for submission of relevant documents or financial statement as the case may be.

xi. No transaction or account-based relationship is undertaken without following the CDD procedures.

xii. Information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or other purposes. It should be ensured that the information sought from the customers are relevant to the perceived risk, are not intrusive and are in conformity with the RBI guidelines issued in this regard.
Where Permanent Account Number (PAN) is obtained, the same shall be verified from all the available legitimate resources.

xiii. Branches should not insist to customer for introduction at the time of opening of account to avoid inconvenience. However, they take introduction if they feel necessary.

While adopting/ implementing all above guidelines/ procedures, Bank shall ensure that banking/ financial facility shall be made available with due care to the general public and specially those who are financially or socially disadvantaged and Persons with Disabilities (PwDs).
The bank shall ensure that no application for onboarding or periodic updation of KYC is rejected without due consideration. The reason for such rejection must be properly recorded by the concerned officer.

xiv. While opening Current Account in branches, Branch Managers or Passing Officers should insist on a declaration from the account-holder to the effect that the firm is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by him with any other bank(s). Branches should ascertain all the details and should also inform the concerned lending bank(s). In case customer having any credit facility in other bank then branches should obtain No-objection Certificate from such banks.

xv. Customers are bound to submit legitimate and true documents at the bank and an employee(s) designated is/are take all efforts to check the genuineness and correctness of the submitted documents.

xvi. **Non submission of PAN**
"For existing customers, the Bank shall obtain PAN or equivalent e-document thereof or Form 60 within the time prescribed by the Central Government. In case of non-submission within the prescribed time, the Bank shall temporarily cease operations in the account until compliance is completed. Where a customer provides a written request refusing to submit PAN or Form 60, the Bank shall close the account after establishing the identity of the customer and settling all outstanding obligations. Temporary ceasing of operations shall mean suspension of all transactions in the account; however, in case of loan or other asset accounts, only credit transactions shall be permitted during such period."

Accounts of Politically Exposed Persons (PEPs)

Branches should not open accounts of PEPs without prior approval of Head Office. Head Office should do below due diligence before permitting to branch to open account of PEPs.

a. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
b. the identity of the person shall have been verified before accepting the PEP as a customer;
c. the decision to open an account for a PEP is taken at a senior level in accordance with the bank Customer Acceptance Policy;
d. all such accounts are subjected to enhanced monitoring on an on-going basis;
e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship; These provisions also extend to family members or close associates of PEPs.
f. At the time of account opening and doing Re-KYC branches should verify whether customer is politically exposed person. Also check any Beneficial Owner is politically exposed person.
g. The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

Opening account of Married Woman:

While opening an account of married woman if no OVD is available in the married name or updated address then branches take the following documents for Proof of Identity and proof of address for change in name and change in address.

1. OVD in maiden name
2. Marriage certificate or Gazette Notification
3. Affidavit(declaring name and address change)
4. Utility bill in husband's name as deemed proof of address
5. Self-declaration of current address (for address change)

For Periodic updation of Married women: If updated OVD is not available then branches may take the following document for periodic updation of kyc

1. Old OVD
2. Marriage certificate
3. Husband's documents (for address)
4. Self-declarations

Money Mule Account – A money mule account is a bank account used by criminals to launder illicit funds by having an individual receive and transfer stolen money on their behalf. The account holder, or "money mule," may be an unwitting victim or a complicit partner in the scheme.
Enhanced due diligence (EDD): The institution shall apply Enhanced Due Diligence measures to customers classified as high-risk, including but not limited to:

- Individuals whose online behavior and professional profile do not align with their transactional activity.
- Clients receiving funds from or sending funds to high-risk jurisdictions.
- Accounts of individuals known to have affiliations with high-risk industries or activities.
- The proper procedure for escalating and reporting suspicious activity.
- How to respond to customers whose accounts are flagged as potential money mules

Activation of Inoperative Account:

If there were no any customer induced transaction in the saving or current account continuously for last 2 year the said account(s) will be classified as an Inoperative Account. No transactions will be allowed in such accounts till the submission of fresh KYC by the account holder(s). Irrespective of the mode of operations in the account fresh KYC of all the holders in the account shall be obtained. Regular monitoring on the inoperative accounts should be exercised which it to be continued for further 6 months from the date of activation of inoperative accounts. Facility of account activation must be provided at all the branches and locations of the bank and ensure that, customer can submit the documents at any of the bank branch irrespective of its Home Branch.

Unique Customer Identification Code

Under Unique Customer Identification Code (UCIC) a customer should have only one client ID in a Bank. UCIC or allotting of unique identification number to each customer, help banks to identify customer, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers including setting up of a Centralized KYC Registry.

The Bank has implemented UCIC while opening new accounts of fresh customers as well as for the existing customers. Branches should search customer number while opening new account whether there is any existing Customer ID present in the system. If the positive confirmation match then branch should not open new Customer ID in the system, they should using existing.

B) Risk Management

Assessing risk and its management is one of very crucial process for any financial institution. To address risk management the customers are classified into 3 categories i.e Low Risk, Medium Risk and High Risk. Risk categorization shall be based on parameters such as customer constitution, type of customer, identity of customers, financial behavior, nature of business activity, business profile, income source and nature of transactions as mentioned in the **Annexure I**

The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer. Bank should deploy latest technology for risk identification, STR Alert generation etc. Bank shall implement comprehensive customer risk rating policy in the CBS.

Customer Risk Rating Policy:

Customer Risk rating policy is based on Customer profile and customer Transaction

There are basically three types of risk defined the Customer Risk Rating Policy that is KYC, Profile and Transaction.

1) **KYC:**
   KYC section contain Identity proof and Address proof and both having Risk weight 1.If any customer having both Identify proof and address proof then that customer risk weight is 1. KYC segment is only for KYC compliance.
2) **Profile:**
   Profile Risk section contains category of customer and accordingly profile risk weight is associated with it. Ex. If customer is Trust then his risk weight is 3 means High.
3) **Transaction:**
   Transaction sections contains different types of transactions which are based on STR rules and having 3 risk weight.

Low Risk	**:**	**Risk weight 1**
Medium Risk	**:**	**Risk weight 2**
High Risk	**:**	**Risk weight 3**

Customer risk rating policy is defined in Annexure II

Periodic Updation

Bank shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. Updation of KYC is to done for Customer ID level and not for Account Level.
Individual customer who is categorizes as low risk, bank shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or up to June 30, 2026, whichever is later. Bank should monitor these accounts on regular basis.
Bank should intimate the customers for submission of fresh KYC documents, whose date of KYC is due in next 90 days. Minimum 3 intimation should be given to the customer which include at least 1 written intimation. Branches should take all efforts to reach to the customer for updation of KYC. In case where due date of the submission of KYC is already over, bank should give minimum 3 intimations including 1 written intimation to customers to alert them about imposition of transactional restriction in the accounts.

Acknowledgement to customer
"The Bank shall acknowledge receipt of documents/self-declaration submitted by the customer for KYC updation/periodic updation, mentioning the date of receipt. The Bank shall promptly update such information in its records and provide an intimation to the customer indicating the date of KYC updation."
Customer Education
"The Bank shall advise customers to submit updated KYC documents in case of any change in the documents previously furnished, within 30 days of such change, to enable timely updation of records."
"The Bank shall inform customers in advance for periodic updation of KYC. Prior to the due date, the Bank shall issue at least three advance intimations at appropriate intervals, including at least one intimation by letter, through available communication channels. If customers fail to comply by the due date, the Bank shall issue at least three reminders at appropriate intervals, including at least one reminder by letter. Such intimations/reminders shall include simple instructions for KYC updation, details for seeking assistance, and the consequences of non-compliance. All intimations and reminders shall be properly recorded in the Bank's systems for audit trail. The Bank shall implement this process on priority, but not later than January 01, 2026."

a) Individual Customers:

No change in KYC information:
In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained. Customer may submit physical application at any branches of the bank

irrespective of his/her home branch or can send a e-mail to the branch from his/her registered email address.

Change in KYC information:

In case any changes like address, demographic details, ownership, change of business activities etc. is/are observed in the KYC information of an individual, branch is required to obtain full KYC as per process and make necessary changes in the CBS (as applicable).

Address of the customer can be classified into 2 categories

i) **Permeant Address – As mentioned on the OVD**

ii) **Communication Address – As declared by the customer. Though there is no need of submission of proof of communication address, branch should obtain self-declaration from the customer and perform address verification on the communication address of the customer to confirm the genuineness of the customer address.**

Minor turned Major:

Every customer category under Minor and turning to Major should mandatorily submit fresh KYC at the branch to update the status as Major. Minimum 3 intimations/ alerts informing submission of fresh KYC to be given to the customers atleast 30 days prior to he/she turning major Minimum 1 written intimation to be send to the customer's registered address and bank may use alternate digital channels like SMS or Email to send intimation to the customers. Branches should take continuous follow up and collect the required documents from the customers, however conversion of Minor to Major should be updated in the CBS on or after the date of completion of 18 years of age of the customer. Branches should guide the customer regarding benefits of timely submission of documents for Minor to Major conversion.

If customer fails to submit fresh KYC on or before he/she turned Major, customer may not be able to do transaction in the accounts associated with that customer id. Once the fresh KYC will be submitted the transactions in these accounts will be resumed.

b) Customers other than individuals:

No change in KYC information:

Self-declaration for no change in KYC information can be accepted from the legal entity provided branch should exercise due diligence as below:

1. Branch official should visit the registered address of the legal entity and ascertain the correctness with address available in bank record.
2. Confirm the business activity should be in line with the activities mentioned on the proof of legal entity.
3. Confirm the owner or beneficial owners of the legal entities are the same as available in the bank record.
4. CKYC number is generated and updated in the customer ID of the legal entity.
5. All the linked customer id(s) are KYC compliant and CKYC numbers are available in the bank record.

If all efforts taken by branch to confirm the no changes in the KYC information then only Periodic Updation of KYC can be done on the self - declaration duly signed by the authorized signatories or signatories as per the mode of operation only.

Change in KYC information:

In case any changes like address, demographic details, ownership, change of business activities etc. is/are observed in the KYC information of the legal entity, branch is required to obtain full KYC as per process and make necessary changes in the CBS (as applicable).

b) Additional measures:

In addition to the above, branches shall ensure that, 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 branches are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

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 updation/ periodic updation.

At the time of updation/periodic updation of KYC bank shall ensure that the information/ documents collected from the customers should updated in the CBS and an intimation, mentioning the date of updation of KYC details is provided to the customer through SMS.

Bank shall advice the customers that in case any update in the KYC documents submitted by the customer at the time of establishment business relationship/account-based relationship customers should submit the updated documents to the bank within 30 days of the date of updation.

Periodic Review of Customer Risk Categorization

Periodic customer risk rating review is an important aspect of risk management. The objective of this review is to ensure that the bank's customer risk rating process is accurate, consistent, and effective in identifying and managing customer risk. Review is basically depending on the customer category, CTR, STR and KYC component. This review shall take place at least once in six months. Risk review shall be conducted on the basis of customer data on 31st March and 30th September every year. Customer risk categorization to be conducted on Customer ID level on the basis of constitution of customer, occupation of customer, customer profile, business profile, transaction in the linked accounts etc.

On the basis of the review of customer risk categorization Branches should take follow up with the customers for submission of the fresh KYC documents. Bank and branches to maintain privacy of risk rating of the respective customer and should not be disclosed to the customers.

Irrespective of the risk category of a customer, branch may ask fresh KYC if transactions in the account are found suspicious or not in line with the customer profile.

Customers due diligence measures:

Customer due diligence is an important aspect in all the stages of KYC. Customer due diligence may restrict the customer to use the account purely for legitimate purposes. Customer due diligence includes collection of following information to define the customer profile:

i. Correctness of customer KYC documents
ii. Permanent and communication address
iii. Occupation
iv. Source of Income
v. Networth or financial strength of the customer
vi. Expected turn over in the account
vii. Monitoring of account transactions etc.

On the basis of proper customer due diligence branch / bank can come to the decision on risk of customer acceptance and could decide to accept or reject the customer for on boarding. However, customer due diligence shall be a continued process to assess the customer risk.

In case noncompliance of KYC requirements by the customers despite repeated reminders by branch, it has-been decided that branch should impose "partial freezing "in case of such KYC non- compliance in a phased manner. Meanwhile, the account holders can revive account by submitting the KYC DOCUMENTS As per instructions in force. While imposing 'partial freezing ', branches advised to insure that the option of partial freezing is exercised after giving due notice of three months initially to the customers to comply with KYC requirements and followed by a reminder for further period of three months. Thereafter, branches may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are, still KYC non-compliant after six months of imposing initial 'partial freezing' branches may disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the bank to close the accounts of such customers.

The certified copy of the each OVD shall be obtained by the comparing with original OVD so produced by the client and shall be recorded by writing "Original seen and verified" by the authorized officer

C) **Customer Identification Procedure (C.I.P): -**

Bank shall undertake Customer Identification Procedure in the following cases:

i. On boarding of new customer or commencement of banking relationship by the customer
ii. Periodic Updation of KYC
iii. Opening an account of existing customer
iv. When there is a doubt about the authenticity of customer information
v. When there is a doubt about the authenticity of transaction in the linked accounts

For the purpose of verifying the identity of the customers at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear Tobe connected, or any international money transfer operations, banks may depend on customer due diligence done by a third party, subject to the following conditions:

(a)Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

(b) Bank may have adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
(c) The third party is regulated, supervised or monitored
(d) The third party shall not be based in a country or jurisdiction assessed as high risk.
(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.

Proof of Identity:
This refers to any document that proves the identity of a person or an entity. In case of an individual customer it consists name and photograph of the customer. These documents are generally be used for identification of person or an entity and/or for the purposes like taxation.

Officially valid documents:
These are the specific documents officially notified by the government to serve as proof of identity and / or address. As per latest RBI KYC Master Directions the following are treated as OVDs:

i. Passport
ii. Driving License
iii. Voter ID Card
iv. Aadhar Card
v. NREGA job card etc.

Officially valid documents must contain identity and address of the customer and can be used as KYC purposes.

- List of documents for opening saving account mention in Annexure III.
- List of documents for opening current account mention in Annexure IV

Branches should not accept KYC documents from any social media accounts like WhatsApp, Telegram etc, however bank can opt for alternate avenues or resources like Digital Account Opening solutions, Business Correspondence etc for Opening of account or updation of KYC. Branch officials should verify the documents from the original and evidenced the same on the copies of the documents (Original Seen and Verified) in case of physical / offline account processing or to be authenticate digitally in case of digital platform.

Identification of Beneficial Owner (BO)

For opening an account of a Legal Person who is not a natural person, branches should identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) to verify his identity, As per guidelines provided below

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 persons, has/have a controlling ownership interest or who exercise control through other means.

- Controlling ownership interest means ownership of/entitlement to more than 10 percent of the 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.

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/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

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/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

i. Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d) 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 10 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.

e) Declaration of beneficial ownership is to obtained from the customers as per Annexure -V

f) The same to be recorded in the CBS.

D) Monitoring of Transactions: -

Transaction:

Transaction means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a) Opening of an account;
b) Deposit withdrawal, exchange or transfer of funds, whether in cash or by cheque, payment order or other instruments or by electronic or nonphysical means;
c) The use of a locker or any other form of deposit;
d) Entering into any financial and non-financial relationship which would be fund based or non-fund based;

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

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

Branches will undertake on-going due diligence of customers to ensure that their transactions are consistent with the Bank's knowledge about the customers, customers" business and risk profile; and the source of funds.

Bank has been implemented Anti Money Laundering software and accordingly rules in the software alerts will be generated. For working in software below roles should be assigned to employee for effective working.

1) **Branch Manager Role– Employee working on alerts at branch level should be given Branch Manager AML role.**
2) **MLO (Money Laundering Officer) – Employee working at Head Office and controlling working of AML software is assigned MLO role.**
3) **MLRO (Money Laundering Reporting Officer) – Principal officer of the bank will be given MLRO role in AML software.**

Software will run rules on daily and monthly basis and accordingly alerts will be generated. Branches will whitelist or escalate generated alerts. If particular transaction escalate to HO then MLO will do proper due diligence of escalated transition and if that is really suspicious then MLO will escalate it further to MLRO. MLRO will also do all the due diligence and if that is really suspicious then MLRO will generate STR report and submit on FINGATE 2.0 portal of FIU-IND.

The following types of transactions shall necessarily be monitored:

a) Large and complex transactions including RTGS/NEFT transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

b) Transactions, which exceed the thresholds prescribed for specific categories of accounts.

c) High account turnover inconsistent with the size of the balance maintained.

The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

Ongoing monitoring is an essential element of effective KYC/AML procedures. Branches should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

(a) The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensify monitoring.

(b) Branches should pay particular attention to the following types of transactions:

(i) Large and complex transactions and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

(ii) Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

(iii) High account turnover inconsistent with the size of the balance maintained.

(iv) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

(c) Periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers shall be carried out at a periodicity at list once in six months.

(d) Enhanced Due Diligence (EDD) is a, **risk-based process** used by banks and financial institutions to **verify the identity and activities of high-risk customers or transactions**.

EDD is applicable to Non-Face-to-Face Customer Onboarding, High-Risk Customers, and Existing Customers Becoming High-Risk.

Periodical review can be done on the basis of customer's transaction alert generated, CTR generated and customer category.

(e) Branches should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies (If branches having these type of accounts). Branches should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the branches and in case they find such unusual operations in their

accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

e) Branch Managers / Passing Officers should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt, make necessary enquiries with the account holders.

f) Branches are advised to mandatorily obtain either PAN for opening of accounts. If customer is not having PAN then Form 60 may take and time of account opening and whenever customer did transactions equal or more than 50000/- Branches should send these form 60 to Tax Department over email for the purpose of Form 60 return to Income Tax.

g) All the staff members are instructed to maintain the standards of good conduct and behaviour expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

h) Cash transaction more than 5 lack should be monitor at branch.

As per master circular and subsequent directions issued by the Reserve Bank of India bank may opt for following alternative channels for KYC Compliance.

OTP based e-KYC

Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

- There must be a specific consent from the customer for authentication through OTP.

  As a risk-mitigating measure for such accounts, bank shall ensure that transaction alerts, OTP, etc., are sent only to registered mobile number of the customer linked with Aadhaar. Bank shall have a board approved policy for dealing with requests for change of mobile number in such accounts.

- The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
- The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-

CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

- If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.
- **As a risk-mitigating measure for such accounts, bank shall ensure that transaction alerts, OTP, etc., are sent only to registered mobile number of the customer linked with Aadhaar. Bank shall have a board approved policy for dealing with requests for change of mobile number in such accounts.**

V-CIP Procedure:

Bank may undertake V-CIP to carry out:

CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28, apart from undertaking CDD of the proprietor.

Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

Updating/Periodic updating of KYC for eligible customers.

Bank opting to undertake V-CIP, shall adhere to the following minimum standards:

a) V-CIP infrastructure

b) V-CIP procedure

Bank opting to undertake V-CIP, shall adhere to the RBI's standard mentioned in KYC Master Direction's section 18(a) V-CIP infrastructure.

Secrecy Obligations and Sharing of Information:

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

(b) While considering the requests for data / information from Government and other agencies, bank 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 banking transactions.

(c) 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 bank requires disclosure and

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

(d) 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

IMPLEMENTATION

1) Adherence to Foreign Contribution Regulation Act (FCRA) 1976:-

Branch Manager should adhere to the instructions on the provisions of the Foreign Contribution Regulation Act 1976, regarding opening of accounts and collecting the cheques only in favour of associations, which are registered under Foreign Contribution Regulation Act. A certificate to the effect that the association is registered with Government of India should be obtained from concern associations at the time of opening of the account or collection of cheques.

Branch Managers are inform that they should not open accounts of banned organizations the names of which are advised by Reserve Bank of India from time to time.

As per Foreign Account Tax Compliance Act bank should submit yearly report called FATCA.

However, Sundarlal Sawji Urban Co-op Bank Ltd. is not authorized to deal in foreign exchange.

1) Internal Control:-

To follow the Know Your Customer procedure properly, duties & responsibilities of the officers and employees have been defined as under:-

a) The payments and deposits of cheque above Rs.25,000/-should be scrutinize properly.

b) Blank cheques, Demand Draft, Pay Orders should be kept in lock and key and proper register should be maintained and Branch manager should submit the report in that connection on quarterly intervals.

c) The Inoperative/Dormant accounts should be allowed to be operated by the Branch Manager only after getting satisfactory compliance.

d) At the time of issuing cheque book officer should verify the identity of the account holder.

e) Branch Manager must inform immediately to Central Office about the lost cheque, demand draft and pay orders.

2**) Record Keeping:-**

- Branch Manager should ensure proper record keeping of the transactions of the customer.
- Branches have to maintain necessary records of transactions of the customers, for at least five years from the date of transaction.
- **Branches have to preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during of business relationship, for at least five years after the business relationship is ended.**
- Branches should preserve record such that record will quickly available regarding the identification records and transaction data to the competent authorities' upon request.
- Maintain proper record of transactions as prescribed under Rule 3 of prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules 2005)
- Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
- The nature of transaction
- The amount of transaction and the currency in which it was denominated.
- The date on which the transaction was conducted; and
- The parties to the transaction
- Branches have to maintain records of the identity and addresses of their customer, and records in respect of transactions referred to in Rule3 in hard or soft copy format.
- Bank 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, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the bank has ended or the account has been closed, whichever is later.

3) **Training to Staff:-**

Head Office has taken initiative to provide ongoing training to staff; so that they can understand their duties and responsibilities in complying the KYC and anti-money laundering guidelines and implementing Know Your Customer Policies. **Staff working in Deposit section or KYC and CKYC at branch level should be given training as and when required.**

4) **Obligation to maintain confidentiality:-**

The information collected by the Bank in respect of the customers while complying with the Know Your Customer Guidelines, should be kept confidential and should not be provided to any private agencies.

5) **Appointment of Designated Director and Principal Officer:**

The Bank shall appoint a Designated Director and a Principal Officer for the purpose of ensuring compliance with the provisions of the Prevention of Money-laundering Act, 2002, the rules framed thereunder, and the Reserve Bank of India Know Your Customer (KYC) Directions, as amended from time to time.

The Bank shall ensure that the Designated Director and the Principal Officer are two separate and distinct individuals. The Designated Director shall be responsible for overall compliance with AML/CFT obligations at the Board level, while the Principal Officer shall be responsible for day-to-day implementation, monitoring and reporting under the AML/CFT framework.

The name, designation, office address, email ID and contact number of the Designated Director and the Principal Officer shall be intimated to the Reserve Bank of India and FIU-IND in the prescribed manner. Any change in the appointment or contact details of either official shall be promptly communicated to RBI and FIU-IND without delay.

6) Central KYC Record Registry (CKYCR)

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

Bank should capture customers KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

Bank should capture the KYC information for sharing with the CKYCR, as per the KYC templates prepared for 'Individuals' and 'Legal Entities'as the case may be.The template may be revised from time to time as may be required and released by CERSAI.

Bank shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021and all new individual accounts opened on or after from April 1, 2017 with CKYCR.

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

An entity defined under rule 2(1) (a) of the Rules, to receive, store, safeguard and retrieve the record of KYC records in digital form of a customer.
Bank need to complete C-KYC procedure of new customer very next day from account base relationship with bank and existing customers also. Unless customer did not complete CKYCR process, he cannot avail banking facilities.

Also, whenever the bank obtains additional or updated information from any customer the bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records Of the existing customer in CKYCR.CKYCR then informs electronically all the reporting entities regarding updation of KYC record of the said customer. Then CKYCR informs to bank regarding an update in the KYC record of an existing customer, the bank shall retrieve the update KYC record from CKYCR and update the KYC record maintained by the bank

To establish an account-based relationship, update customer details, or verify identity, the bank shall obtain the KYC Identifier from the customer or retrieve it from the Central KYC Registry (CKYCR) and use it to access KYC records online. The customer should not be asked to resubmit the same KYC documents or provide additional ID, unless:

1. There is a change in the customer's information in CKYCR;
2. The retrieved KYC data is incomplete or not as per current norms;
3. The validity of the downloaded documents has expired; or
4. The bank finds it necessary for identity/address verification, enhanced due diligence, or risk profiling.

Use of CKYCR Records for Customer Due Diligence

Wherever applicable, the Bank shall rely on the customer's KYC records available in the Central KYC Records Registry (CKYCR). The Regulated Entity that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verification of the customer's identity and/or address, as applicable. Accordingly, upon downloading and relying on such KYC records from the CKYCR, the Bank shall not be required to re-verify the authenticity of the customer's identity and/or address, provided that the KYC records so downloaded are current and are in compliance with the provisions of the Prevention of Money-laundering Act, 2002 and the Prevention of Money-laundering Rules, 2005. Notwithstanding the above, the Bank shall remain fully responsible for compliance with all aspects of the Customer Due Diligence (CDD) process and the provisions of the Reserve Bank of India Know Your Customer Directions, as amended from time to time, except for the verification of identity and/or address of the customer to the extent such verification has already been carried out by the Regulated Entity that last updated the KYC records in the CKYCR.

Flagging of Deceased Customers in CKYCRR

Upon receipt of reliable information and valid documentary evidence confirming the death of a customer, the Bank shall promptly update the customer's KYC record in the Central KYC Records Registry (CKYCRR) by flagging the KYC status as "Deceased".

The update shall be carried out through the CKYCRR KYC updation process by capturing the date of demise, documentary evidence, and remarks, if any, in the designated "Other Details / Deceased Information" field, in accordance with the guidelines issued by the Central KYC Records Registry.

Once a KYC record is flagged as "Deceased" in CKYCRR, the Bank shall ensure that such KYC records are not relied upon for any fresh customer due diligence or on boarding purposes. The Bank shall also take note that such records will not be available for download from CKYCRR and shall be identifiable only through search responses with a distinct identifier, as prescribed by CKYCRR.

The Bank shall maintain proper records of documentary evidence supporting the updation and ensure that necessary system and procedural controls are in place to prevent misuse of accounts or services of deceased customers.

AML Policy.

The major objectives of the policy are:

To prevent the bank accounts and banking services from being used intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

To create awareness about legal and regulatory frame work for AML/CFT requirements and systems among staff.

To interpret the obligations under the PMLA and other relevant regulations and how they may be implemented in practice,

To align the banking operations with good international industry practice in AML/CFT procedures through a proportionate risk based approach, and

To implement the systems and controls necessary to mitigate the risks of the Bank being used in connection with money laundering and terrorist financing.

To meet the statutory requirements under PMLA, Bank has constituted an AML (Anti Money Laundering) Cell under the control and supervision of Principal Officer comprising senior and trained officers including IT support officers. Bank has implemented AMLKYC software for alert generation. The functions of the AML Cell are as follows:

To analyze the alerts generated through AML software System based on IBA recommended parameters for STRs, prepare notes and to get it approved by the Principal Officer.

To generate monthly cash Transaction Report (CTR) and Non-Profit Organization Report (NTR).

To file the Counterfeit Currency Report (CCR) after receiving from Security Department within time schedule to FIU-IND.
To adopt suitable steps to procure any information about the customers or transactions which the Regulatory Authorities require.

To inform all the branch level functionaries about the day to day matters developed relating to national and international findings of the countries with Inadequacies in their approach for prevention of money laundering.

What is Money Laundering?

The offence of Money Laundering has been defined in Section 3 of the Prevention of Money Laundering Act (PMLA), 2002 as "who is 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".

"Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds.

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity-

- **Placement** - the physical disposal of cash proceeds derived from illegal activity.

- **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

- Integration – placing the laundered proceeds bank into the economy in such a way that they re-enter the financial system appearing to be normal business.

Proliferation Financing (PF)
The Bank shall establish internal controls to identify, assess, monitor and mitigate the risks arising from Proliferation Financing (PF), in line with the provisions of the Prevention of Money-laundering Act, 2002, applicable rules, and the Reserve Bank of India Know Your Customer (KYC) Directions, as amended from time to time.
The Bank shall undertake screening of customers, beneficial owners, counterparties and transactions against sanctions lists, watch lists and advisories issued by the United Nations

Security Council (UNSC), the Government of India, the Reserve Bank of India, and such other competent authorities, at the time of on boarding and on an ongoing basis.
The Bank shall implement enhanced monitoring mechanisms for trade-related transactions, including transactions involving high-risk jurisdictions, sensitive goods, complex trade structures or unusual payment patterns, with a view to detecting indicators of Proliferation Financing.
The Bank shall ensure that alerts, red flags and unusual patterns suggestive of Proliferation Financing are promptly examined, appropriately escalated to the AML department at HO (Principal Officer), and reported to FIU-IND and other authorities, wherever required, in accordance with applicable regulatory and legal requirements.
Periodic trainings should be provided to its staff to enhance awareness of Proliferation Financing risks, typologies and red flag indicators, and shall review and update its PF risk mitigation framework at regular intervals or upon issuance of new regulatory or governmental instructions.

1) **Functions of Branches regarding KYC-AML.**

Branch officials play vital roles on compliance of KYC norms and assist to prevent money laundering. Branches functions concerning with KYC-AML norms can be classified as follows.

Follow the KYC Policy of the Bank and circulars issued from time to time pertaining to KYC-AML, exercise of CDD (Customer Due Diligence) and EDD (Enhanced Due Diligence) while opening of new accounts.

i) Monitor transaction on daily basis especially dormant account's transactions.

ii) Making KYC updating of all old non KYC compliant accounts, observing all KYC norms within time schedule. It is to be ensured that the pertinent aspects of customer's identity like communication & permanent address, occupation, PAN etc. are properly incorporated in the CBS system under customer master.

iii) Detection and Impounding of Forged Indian Currency Notes (FICN) by the staff engaged in handling of cash in the branches/currency chests and reporting the same to the Security Department, Head office.**by7thof the succeeding month** positively, so that the centralized AML Cell may report to FIU-IND by 15th of the same month.

Earlier branches were required to file FIR in case of each detection of counterfeit note irrespective of the number of pieces and bonafides of the tenderer. Now the matter has been reviewed by RBI and it has been decided that for detection of counterfeit notes up to 4 (four) pieces in a single transaction, a consolidated report per month to be sent but for detection of counterfeit notes of five or more pieces in a single transaction, FIR should be lodged with Nodal Police Station / Police Authorities as per jurisdiction.

iv) Proper maintenance of records of all transactions and documents relating to KYC norms.

v) Maintaining secrecy about the transactions of accounts under monitoring for suspicious activities.

Reporting is an obligation of suspicious transactions relating to money laundering or terrorist financing activities. All branches are required to report any suspicious activities observed by them which is still under doubt after taking the due diligence, immediately to their Chief Regional Manager under 'confidential' cover which in turn will immediately be sent with observation to the Principal Officer for taking final decision and filing the Suspicious Transaction Report to FIU-IND based on 27 **'Indicative Alert Indicators for Branches /Department.**

2) Reporting Obligation under PMLA .

In terms of the Rules notified under Prevention of Money Laundering Act (PMLA), 2002, certain obligations were cast on banking companies with regard to reporting of certain transactions. The RBI has issued guidelines detailing the obligation of banks in term of the Rules notified under PMLA.

Accordingly, Bank is required to make the following reports to the FIU-IND.

1. Cash Transaction Reporting (CTR)
2. Counterfeit Currency Reporting (CCR)
3. Suspicious Transaction Reporting (STR)
4. Non-Profit Organization Reporting (NPOR/NTR)

2.1 Cash Transaction Reporting (CTR).

As per the PMLA rules, Bank is required to submit the details of:

- They are in Cash
- All the transactions are of same nature (i.e. Either Credit or Debit), that is the receipts and the payments from the customer are considered separately.
- All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.

- All series of cash transactions integrally connected to each other, which have been **individually** valued below rupees ten lakh or its equivalent in foreign currency, where such series of transactions have taken place within a month and the monthly aggregate exceeds rupees ten lakh or its equivalent in foreign currency.

  For integrally connected cash transactions, total debit and total credit in a month should be considered separately. However, the bank should not separately report to FIU-IND which is less than Rs.50, 000.00.

  This report is required to be filed on a monthly basis by 15th of the succeeding month.

2.2 Counterfeit Currency Reporting (CCR)

The PMLA Rule 3(1)(C) read with rule VIII requires the reporting of all cash transactions where forged or counterfeit Indian currency notes have been used as genuine. **The reports required to be filed by the 15th day of the succeeding month for centralized AML Cell.**

The consolidated monthly report of the branch should be sent to KYC department, at Head Office, Jintur **within the 7th day of the succeeding month and KYC Department in turn send the consolidated monthly report immediately to centralized AML Cell for onward filing to FIU-IND.** While submitting the report of FICN to HO, they should specifically mention Date of detection and denomination wise currency Serial Nos. Bank should submit CCR report to RBI Issue Department (Soft copy), Department of Economic Affairs (Hard Copy), and National Crime Records Bureau (NCRB) to 7thday every of months.

2.3 Suspicious Transaction Reporting (STR)

As per PMLA Rule 2(g) Suspicious Transaction means a transaction whether or not made in cash which to a person acting in good faith –

a. gives rise to 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 bonafide purpose gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

(i) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents .Bank will report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.

(ii) Bank to submit STRs if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iii) Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

(iv) Bank will ensure not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.

(v) The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions.

2.4 Not-Profit Organization Report (NTR)

The report of all transactions involving receipts by non-profit organizations of value more than Rupees ten lakh or its equivalent in foreign currency should be submitted every month to FIU-IND by 15th of the succeeding month in the prescribed format.

3.3.1 Generation of Alerts

Alert generation involves application of scenarios and risk factor to detect potentially suspicious activity. Effective alert generation is very critical to the quantity and quality of the STRs generated by the bank. Indicators are circumstances that indicate suspicious nature of transactions. Suspicious transaction may be detected from one indicator or a set of indicators.

In the new reporting format specifications, the bank are required to provide information about the source of alert and the alert indicator(s) for detection of suspicious transactions. Our bank has adequate processes and systems for detection of transactions and reporting of suspicious transactions, identified by the employee at Branches/Departments and are using centralized Alert Generation Software-AML SOFTWARE, based on IBA recommended parameters.

In AML software alert will be generated mention in Annexure VI

Procedure of STR Alerts Scrutiny:

Step 1 : Daily/Monthly Alert Review by Branch
Branches must review the alerts generated in the AML software **on a daily or monthly basis**, as per defined frequency.
Each alert must be reviewed with attention

- Customer occupation/Nature of Business
- KYC Compliance Status

- Type, amount and patterns of the transaction

Step 2 : Decision by Branch: Whitelist or Escalate

If the alert is found genuine (no suspicious activity):

The alert must be **whitelisted** in the AML system with a **clear, proper remark** and justification

If the alert is found suspicious

The alert must be Escalate to Ho with detailed reason for suspicious.

Step 3: Decision by MLO:

If particular transaction escalate to HO then MLO will do proper due diligence of escalated transition and if that is really suspicious then MLO will escalate it further to MLRO.

Step 4: Decision by MLRO

MLRO will also do all the due diligence and if that is really suspicious then MLRO will generate STR report and submit on FINGATE 2.0 portal of FIU-IND.

3.3.2 Identification of Suspicious transactions by Branches/Departments

There are certain types of transaction which can be identified at the branches/operations departments themselves. The identification of suspicious transaction at Branches/Departments is more likely to be related with the following sources:

- **Customer Verification:** Detected during customer acceptance, identification or verification (excluding reasons mentioned on other codes e.g. use of forged ID, wrong address etc.)
- **Law Enforcement Agency Query:** Query or letter received from LawEnforcement Agency (LEA) or Intelligence Agency (blocking order received, transaction details sought etc.)
- **Media Reports :** Adverse Media Reports about customer (e.g. newspaper reports)
- **Employee Initiated:** Employee raised alert (e.g. behavioral indicators such as customer had no information about transaction, attempted transaction etc.)
- **Public Complaint:** Complaint received from public (e.g. abuse of account for committing fraud etc.)
- **Business Associates:** Information received from other institutions, subsidiaries or business associates (e.g. cross-border referral, alert raised by agent etc.)

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

- Large Cash Transactions
- Multiple accounts under the same name
- Placing funds in term Deposits and using them as security for more loans

- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts
- Money is credited from different locations into an account and immediately withdrawn.
- Money credited / transaction observed in the account is inconsistent with the profile of the customer.
- There is a continuous flow of credit in cash and money is immediately transferred to another account, either in our bank or some other Bank of the same party or of related party.
- There is high activity of credit or debit in newly opened accounts.
- There is sudden high activity or huge cash deposits in an in-operative accounts.

Audit and Inspection of KYC/AML

Concurrent and Internal auditor shall responsible to inspect and find out lacuna in the KYC/AML related working. Risk categorization, Risk review, AML software transactions whitelist/escalations. Reporting to FIU_IND etc. should be checked by Auditor.

Money Laundering and Terrorist Financing Risk assessment by Bank

a) As per Section (5A) of Chapter II of the MD on KYC 2016, the Bank is required to carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with bank from time to time.

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

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

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

The policy stipulates Three Lines of Defence while implementing KYC-AML guidelines these shall be helpful in strengthening the procedures at operational level and shall provide tools for ensuring enough robustness to the entire mechanism at Bank level.

First Line of Defence: The policy shall provide the relevent guidelines and directions from regulators to front line staff at all our branches to deal with the customers at the time of on boarding and at subsequent stages.

Second Line of Defence: Head Office and supervisory lines in the branches and controlling offices shall provide necessary support and ensure putting necessary control mechanisms.

Third Line of Defense: The internal auditors conduct independent audit function to assess the compliance level to ensure effective compliance function in the Bank.

Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967
Compliance with United Nations Security Council (UNSC) Sanctions and Asset Freezing

The Bank shall comply with all sanctions, prohibitions and restrictive measures imposed by the United Nations Security Council (UNSC), as adopted and enforced by the Government of India and communicated by the Reserve Bank of India from time to time.

The Bank shall have in place robust systems, procedures and controls to identify and screen customers, beneficial owners, accounts, transactions and counterparties against the applicable UNSC sanctions lists, including at the time of onboarding and on a continuous, ongoing basis.

Upon identification of a match with any designated individual or entity under the UNSC sanctions lists, the Bank shall immediately freeze all funds, financial assets or economic resources held by such individual or entity, without prior notice and without delay, in accordance with applicable legal and regulatory requirements. No funds or assets shall be made available, directly or indirectly, to or for the benefit of such designated persons or entities.

The Bank shall promptly report the details of such freezing actions, including particulars of the customer, accounts, assets frozen and the date of action taken, to the Reserve Bank of India and the Financial Intelligence Unit – India (FIU-IND) within the prescribed timelines, in the manner specified under applicable guidelines and directions.

List of Annexure:

Annexure No	List
Annexure I	Risk categorisation
Annexure II	Customer Risk rating policy
Annexure III	List of documents for saving account
Annexure IV	List of documents for current account
Annexure V	Beneficial ownership declaration
Annexure VI	STR rules
Annexure VII	Customer Due Diligence Form

Annexure I: Risk Categorization

Risk Type	Accounts
1)Low Risk	a. Salaried person accounts, used only for salary purpose. b. Students c. House wives, Pensioners d. GOVT DEPT, GOVT. OWNED COMPANIES e. Small Business, Self Employed f.. Farmers, workers
2) Medium Risk	a. Partnership Firm b. Private Limited Company c. Travel agent d. Business (Hotel, Internet Service Provider, Service Provider, Pharmacist, Physiotherapist etc.) e. Professionals like CA, Advocates, TAX Consultants, Doctors, Engineers, Architect f. Constructions and Real Estate Business g. retail shops
3) High Risk	a. Trust, NGOs, Charitable Organizations b. Society and co-op Credit societies c. Jewelers d. Educational Institution f. Accounts those are operated by agent, professional intermediaries, power of attorney holders, mandatory etc.

	g. Accounts of the politically exposed persons and the accounts of the family members or close relatives of the political exposed persons. h. NRI/NRO i. High Net worth Individuals/Premium Customers g. Limited Liability companies

Annexure II: Customer Risk Rating Policy

RISK TYPE SECTION

Risk Type	weight
KYC	**3**
Profile	**3**
Transaction	**3**

KYC SECTION:

Serial No.	Label Name	Column Value	Weight
1	ID Proof	ID Proof	2
2	Address Proof	Address Proof	2

PROFILE RISK SECTION:

Serial No.	Label Name	Field Column	Column Value	Weight
1	Account Type	account_type	NRE ACCOUNT	3
2	Account Type	account_type	HIGH NETWORTH INDIVIDUAL	3
3	Account Type	account_type	PARTNERSHIP	2
4	Account Type	account_type	PRIVATE LIMITED COMPANY	2
5	Account Type	account_type	LIMITED COMPANY	2
6	Account Type	account_type	TRUST	3
7	Account Type	account_type	SOCIETY	3
8	Account Type	account_type	ASSOCIATION	3

9	Account Type	account_type	GROUP/MANDAL	3
10	Account Type	account_type	HUF	2
11	Account Type	account_type	ORGANISATION	2
12	Account Type	account_type	EDUCATIONAL INSTITUTION	3
13	Account Type	account_type	NGO	3
14	Account Type	account_type	LIMITED LIABILITY PARTNERSHIP	2
15	Account Type	account_type	ESTATE AC	2
16	Account Type	account_type	PATPEDHI/CREDIT SOC	3
17	Account Type	account_type	COMPANY FOR CHARITY	3
18	Account Type	account_type	EDUCATIONAL INSTUTION	3
19	Account Type	account_type	ASSOCIATION OF PERSON	3
20	Customer Organization Type	industry	MANUFACTURING	2
21	Customer Organization Type	industry	DISTRIBUTION	2
22	Customer Organization Type	industry	WHOLESALE	2
23	Customer Organization Type	industry	TRADING	2
24	Customer Organization Type	industry	JEWELLERS	3
25	Customer Organization Type	industry	SERVICE PROVIDER	2
26	Customer Organization Type	industry	IMPORTING	3
27	Customer Organization Type	industry	EXPORTING	3
28	Customer Organization Type	industry	DEALERS	2
29	Customer Organization Type	industry	AADAT	2
30	Customer Organization Type	industry	PETROL PUMP	2
31	Customer Organization Type	industry	PHARMA	2
32	Customer Organization Type	industry	INFORMATION TECHNOLOGY	2
33	Customer Organization Type	industry	HOSPITAL OR HEALTHCARE	2
34	Customer Organization Type	industry	BAR/WINESHOP/LIQURE	3
35	Customer Organization Type	industry	HOTEL/RESTAURANT	2
36	Customer Organization Type	industry	CUSTOMER SERVICE POINT/MULTISERVICES	3
37	Occupation	occupation	DOCTOR	2
38	Occupation	occupation	ADVOCATE	2
39	Occupation	occupation	TAX CONSULTANT	2
40	Occupation	occupation	ARCHITECT	2
41	Occupation	occupation	TRANSPORT OPERATOR	2
42	Occupation	occupation	SOFTWARE CONSULTANT	2
43	Occupation	occupation	BUSINESS	2
44	Occupation	occupation	SELF EMPLOYED PROFESSIONAL	2
45	Occupation	occupation	SPORTSMAN	2
46	Occupation	occupation	CONTRACTOR/BUILDER	3
47	Occupation	occupation	BUSINESSWOMAN	2
48	Occupation	occupation	JWELLERS	3
49	Occupation	occupation	CHARTERED ACCOUNTANT	2

50	Occupation	occupation	PHARMACIST	2
51	Occupation	occupation	AUDITOR	2
52	Occupation	occupation	CUSTOMER SERVICE POINT/MULTISERVICES	3
53	Occupation	occupation	EXPORT/IMPORT	3
54	Occupation	occupation	INTERNET SERVICE PROVIDER	2
55	PEP	pep	PEP1	3

Annexure III:

TYPE OF CUSTOMER	REASONS	DOCUMENTS
For Individual(single or joint)	Proof Of Identification Address proof photograph	**Self-Attested copies of each account holder** A. PAN Card or Form 60 **AND** B. OVD / ID Proof & Address Proof (Any one from below) 1. Aadhaar Card/ UID 2. Valid Driving License 3. Voter ID / NAREGA Card 4. Valid Passport C. Latest Passport size colour photograph
HUF	Proof Of Identification Address proof photograph	**Self-Attested copies of** A. PAN Card (HUF and Karta) **AND** B. OVD / ID Proof & Address Proof of Karta (Any one from below) 1. Aadhar Card/ UID 2. Valid Driving Licence 3. Voter ID / NAREGA Card 4. Valid Passport C. Latest Passport size colour photograph D. Latest passport size colour photograph of KARTA

Minor operated by natural guardian	Proof Of Identification Address proof photograph	**Self-Attested copies of** A. PAN Card / Form 60 of natural guardian of a minor **AND** B. Birth Certificate / UID / Aadhar Card / Passport/PAN card of Minor OVD / ID Proof & Address Proof of Natural Guardian of a minor (Any one from below) 1. Aadhar Card/ UID 2. Valid Driving Licence 3. Voter ID / NAREGA Card 4. Valid Passport C. Latest Passport size colour photograph of Guardian D. Latest Passport Size Photograph of minor
Trust/Society	Name of account holder Address proof	1. Certificate of Registration 2. Certificate under section 12 A of Income Tax Regulation 3. PAN 4. Bye Laws 5. List of Management Committee 6. Declaration of Beneficial Ownership 7. OVD of Authorised Signatories and Beneficial owner a. PAN b. Aadhar c. Voter ID d. Valid Passport e. Valid Driving Licence g .Latest Passport Size photograph of each authorised signatories and Beneficial Owners

Annexure IV:

TYPE OF CUSTOMER	**REASONS**	**DOCUMENTS**
Proprietorship	Name of account holder	**Self-Attested copies of** **A. For Proprietary Firm** 1. Registration Certificate / Udyam Certificate / Food and Drug Licence, Shop Act Licence / GST Certificate **B. For Proprietor** 1. PAN Card 2. Voter ID / Valid Passport / Valid Driving Licence / Aadhar Card **C. Latest passport size colour photograph**
Partnership Firm		**Self-Attested copies of** **A. For Partnership Firm** 1. Partnership Deed (Notarised or Registered) 2. PAN Card of Partnership Firm 3. Registration Certificate / Udyam Certificate / Food and Drug Licence, Shop Act Licence / GST Certificate 4. List of Partners 5. Letter on letter head of the firm for opening of an account along with mode of operation Clause **B. For Partners and Authorized Signatories** 1. PAN Card 2. Voter ID / Valid Passport / Valid Driving

		Licence / Aadhar Card **C. Latest passport size colour photograph**
Company		**Self-Attested copies of** **A. PVT LTD Company** 1. Registration Certificate (ROC) 2. PAN Card 3. MOA and AOA 4. Udyam Certificate / Food and Drug Licence, Shop Act Licence / GST Certificate 5. List of Directors 6. Board Resolution for opening of account along with mode of operation Clause **B. For Directors and Authorized Signatories** 1. PAN Card 2. Voter ID / Valid Passport / Valid Driving Licence / Aadhar Card **C. Latest passport size colour photograph**
Trust/Society		**Self Attested Copies of** **A. Trust / Society** 1. Certificate of Registration 2. Certificate under section 12 A of Income Tax Regulation 3. PAN 4. Bye Laws

		5. List of Management Committee 6. Declaration of Beneficial Ownership 7. Board Resolution for opening of account along with MOP Clause **B. For Trustees/ Directors / Authorised Signatories / Beneficial Owners** 1. PAN 2. Aadhar 3. Voter ID 4. Valid Passport 5. Valid Driving Licence **C. Latest Passport Size photograph of each authorised signatories and Beneficial Owners**
Accounts of juridical persons	Government or its Departments, societies, Universities and local bodies	1) Document showing name of person authorized to act on behalf of the entity. 2)Officially valid document for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and 3) Such documents as may be required by the bank to establish the legal existence of such an entity /judicial person.
Unincorporated association or a Body of Individuals		1) Resolution of the managing body of such association or body of individuals 2) Permanent Account Number of the unincorporated association or a body of individuals 3) Power of attorney granted to transact on its behalf. 4) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

Annexure V: Beneficial ownership declaration

दिनांक:

प्रति,

शाखा व्यवस्थापक,
सुंदरलाल सावजी अर्बन को-ऑप बँक लि., जिंतूर
शाखा:

मी/आम्ही, ---------- येथील ---------- या नात्याने, आमच्या संस्थेच्या खालील Beneficial Ownership ची माहिती देत आहोत.

संस्थेचे नाव: संस्थेचा प्रकार:
नोंदणी क्रमांक / CIN: संस्थेचा पॅन क्रमांक:
नोंदणीकृत पत्ता:

Beneficial Ownership बाबत माहिती

Sr. No	Name of Beneficial Owner	DOB	Address	Percentage of Beneficial Ownership	Position
1.					
2.					
2.					
3.					

टीप: Beneficial Owner म्हणजे:
(i) तो व्यक्ती जो संस्थेवर अंतिम मालकी हक्क किंवा नियंत्रण ठेवतो.
(ii) कंपनीसाठी — ज्या व्यक्तीकडे 10% पेक्षा अधिक शेअर्स किंवा मताधिकार आहेत.
(iii) भागीदारीत — ज्या व्यक्तीला 10% पेक्षा अधिक नफा/भांडवली हक्क आहे.
(iv) ट्रस्टसाठी — कर्ता, विश्वस्त, लाभार्थी यापैकी कोणताही जो 10% पेक्षा अधिक हक्क राखतो.
(v) असंघटित संस्थांसाठी (Unincorporated Association) — 15% पेक्षा अधिक हक्क असलेली व्यक्ती.
सदर माहिती सत्य असून ही माहिती खोटी किंवा दिशाभूल करणारी किंवा चुकीची आढळल्यास याबाबत मला/आम्हाला जबाबदार धरले जाऊ शकते. याबाबत मला/आम्हाला जाणीव आहे.

स्वाक्षरी: _____
नाव: पद:
दिनांक: स्थळ:
संस्थेचा शिक्का

फक्त कार्यालयीन वापरासाठी

सन्माननीय ग्राहकाने सादर केलेली Beneficial Ownership बाबतची माहीती सीबीएस माहे अद्यावत केली आहे.

मेकर श्री: ..... चेकर श्री:
स्वाक्षरी: स्वाक्षरी

Annexure VI: Currently Working Rules

Rule Type	Weight	Rule Name	Rule Description
	3	NPO Rule 1	For non-profit organisations, Society & Trust (Omni AcctTypes: 5 & 13) single txn >= 10,00,000 during the reporting month to be

			identified.
CCR Generated 1	3	CCR Generated	CCR Generated
CTR Generated 1	2	CTR Rule 1	Total Debit Cash Transactions > Rs. 10,00,000/- during the month.
		CTR Rule 2	Total Credit Cash Transactions > Rs. 10,00,000/- during the month.
Defaultor 1	3	Defaulter in BlackLists	Defaulter in BlackLists
STR Generated 1	2	Daily STR 1	JEWELLER ACCOUNT
		Daily STR 2	STAFF ACCOUNT
		Daily STR 3	CASH DEPOSIT BY MULTIPLE SLIPS
		Daily STR 4	PEP CUSTOMER
		Daily STR 5	HIGH KYC RATING CUSTOMER
		Daily STR 6	CASH TRANSACTION OVER 2 LAKH IN NPO or **EDUCATIONAL INSTITUTION**
		Manual STR	Manually Escalation of Transaction
		STR 16	Top 10 Cash Transactions >= Rs. 500000
		STR 17	Top 10 Credit Transaction>= 500000
		STR 18	All transactions of OFAC list customers
		STR Rule 1	Corporate customer's turnover > Rs ~~500000~~ **1000000**.00 and quarterly credit flows in the account is > 50% of the turnover.
		STR Rule 10	Rapid movement of funds
		STR Rule 11	Debit transactions just under the reporting threshold amount (Rs 1000000.00) to avoid reporting
		STR Rule 12	Credit transactions just under the reporting threshold amount (Rs 1000000.00) to avoid reporting
		STR Rule 14	Turnover in month > last quarter average balance
		STR Rule 15	Credits > 500000 in month **for saving account**
		STR Rule 19	Single Credit Transaction exceeding Rs ~~25~~ **50** Lakh in Current Account
		STR Rule 2	Cash deposits >= Rs 500000.00 in a month.
		STR Rule 20	Total Deposit in Current Account >= Rs 1 Cr during the month
		STR Rule 21	Total Cash Deposit or Withdrawal in Current Account >= Rs 25 Lakh during the month
		STR Rule 22	Single Cash Debit ~~or Credit~~ Transaction exceeding Rs 5 Lakh in Current Account
		STR Rule 23	No. of Cash Transactions > ~~20~~ **40** during the month for Current account
		STR Rule 24	Dishonour of deposited cheques in CA exceeding 10 times during the month
		STR Rule 25	Dishonour of issued cheques for CA exceeding 2 times during the month
		STR Rule 27	No. of Transactions > 50 during the month for Saving account

		STR Rule 28	Total Deposit in Saving Account > Rs 25 lakh during the month
		STR Rule 29	Total Cash Deposit or Withdrawal in Saving Account >= Rs 10 Lakh during the month
		STR Rule 3	Total cash deposits during the month is >= Rs 500000.00 and >= 50% of the average cash deposits for the last 3 months.
		STR Rule 30	Single Debit or Credit Transaction exceeding Rs 5 Lakh in Saving Account
		STR Rule 31	Dishonour of deposited cheques in Saving account exceeding 5 times during the month
		STR Rule 32	Dishonour of issued cheques in Saving account 2 times during the month
		STR Rule 4	Transactions of a customer for which total monthly debit is > Rs 500000.00 and cash debit is >= 50% of total monthly debit
		STR Rule 5	Transactions of a customer for which total monthly credit > Rs 500000.00 and cash credit is >= 50% of total monthly credit
		STR Rule 6	Credit transactions of a customer for which total number of credit transactions > 25 credit transactions per day
		STR Rule 7	Large Transaction Exceeding Rs 2000000.00 **in a saving account**
		STR Rule 8	Transactions in inoperative or dormant accounts
		STR Rule 9	High cash transactions in new accounts (2 lakhs & above) in last six months
		STR Rule 9.1	High cash transactions in new accounts (2 lakhs & above) in last six months for SB having limit >=200000
		STR Rule 9.2	High cash transactions in new accounts (2 lakhs & above) in last six months for CD having limit >=500000

Modified rules send for updation :-

Daily :-

Rule Name	Rule Description	Limit
Daily STR 1	HIGH VALUE CASH TRANSACTIONS IN NON-INDIVIDUAL CUSTOMERS ACCOUNTS IN A DAY	RS 5 LAKH AND ABOVE
Daily STR 2	HIGH VALUE TRANSACTIONS BY ANY MODE IN INDIVIDUAL CUSTOMERS ACCOUNT IN A DAY	RS.5 LAKH AND ABOVE
Daily STR 3	CASH DEPOSITED BY MULTIPLE SLIPS	>=5
Daily STR 4	HIGH VALUE TRANSACTIONS IN PEP CUSTOMERS ACCOUNT IN A DAY	RS.5 LAKH AND ABOVE
Daily STR 5	TRANSACTION IN KYC NON COMPLIED/NON PAN CUSTOMERS ACCOUNTS IN A DAY	RS.50000/- AND ABOVE
Daily STR 6	CASH TRASANCTION OVER 2 LAKH IN NPO CUSTOMERS ACCOUNTS IN A DAY	RS 2 LAKH AND ABOVE
Daily STR 7	HIGH VALUE CASH TRANSACTION IN INDIVIDUALS CUSTOMERS ACCOUNTS IN A DAY	RS.2 LAKH AND ABOVE
Daily STR 8	SUDDEN ACTIVITY IN A DORMANT/INOPERATIVE ACCOUNTS	50 THOUNSAND AND ABOVE
Daily STR 9	TRANSACTION THAT DEBIT ONE ACCOUNT AND CREDIT TO 3 MULTIPLE ACCOUNTS IN ANYMODE OR ONE TO MANY TRANSFER	5000 AND AVOVE FUND SEND BY ONE REMITTER TO BY MORE THAN 3 RECEIPIENTS
Daily STR 10	MANY TO ONE TRANSFER	5000 AND ABOVE FUNDS SENDS BY MORE THAN 3 REMITTERS TO ONE RECIPIENTS
Daily STR 10	FREQUENT LOCKER OPERATIONS	NUMBER OF LOCKER OPERATIONS GREATOR THAN 4 TIMES IN A DAYS

Monthly :

Rule Name	Rule Description	Limit
RULE 1	HIGH VALUE CASH TRANSACTION INCONSISTANT WITH PROFILE	CASH TRANSACTION GREATER THAN 50000/- BY CUSTOMER WITH LOW CASH REQUIREMENT SUCH AS STUDENTS,HOUSEWIFE AND MINOR ACCOUNTS
RULE 2	DISHONOUR OF DEPOSITED CHEQUES IN CA EXCEEDING 10 TIMES DURING THE MONTH	10 Times
RULE 3	DISHONOUR OF ISSUED CHEQUES IN CA EXCEEDING 2 TIMES DURING THE MONTH	2 Times
RULE 4	DISHONOUR OF DEPOSITED CHEQUES IN SAVING A/C EXCEEDING 5 TIMES DURING THE MONTH	5 Times
RULE 5	DISHONOUR OF ISSUED CHEQUES IN SAVING A/C EXCEEDING 2 TIMES DURING THE MONTH	2 Times
RULE 6	HIGH CASH TRANSACTION IN NEW ACCOUNTS IN LAST SIX MONTHS FOR SAVING ACCOUNT	>=2 LAKH
RULE 7	HIGH CASH TRANSACTION IN NEW ACCOUNTS IN LAST SIC MONTHS FOR CURRENT ACCOUNT	>=5 LAKH
RULE 8	CURRENT MONTH CREDIT TURNOVER>LAST THREE MONTH TOTAL TURNOVER FOR CORPORATE CUSTOMER	
RULE 9	CREDIT TRANSACTION >=25 CREDIT TRANSACTION FOR SAVING ACCOUNT IN A DAY	>=25
RULE 10	CASH DEPOSIT>=500000.00 IN A MONTH	>=500000

Annexure VII: customer Due Diligence Form

Customer Due Diligence Form - Individual Customer

Branch: _____

Name of the Account Holder	
Account Number	
Customer ID	
PAN Number	
Aadhaar Number / or other OVD Number	
Permanent Address	
Communication Address	
Contact number	
Profession	Salaried / Self Employed / Professional Student / Housewife / Other - _____
Nature of Profession	
Name of the employer / Business	
Address of work place (if any)	
Source of Income	Salary / Business Income / Agricultural Income/ Investment Income
Approx Yearly Income	Rs. _____ Lakh
Approx Net worth	Rs. _____ Lakh
Asset Owned	Moveable Assets: i) Two Wheeler ___ ii) Four Wheeler ___ iii) Other vehicle _____ Immoveable /Fixed Assets i) House – Flat / Independent House – Area _____ Sqft ii) Commercial Property – Area _____ Sqft iii) Open Plot – Area _____ Sqft

I, Mr/Mrs. _____

certified that, the all the above information furnished by me is true with all respect. I solely and wholely be responsible for if any of the information found incorrect.

Date:

Signature of the customer -

Branch Manager Confirmation:

I,
Mr/Mrs._____
physically verified the address mentioned in the account number _____ on dated ____/ _____/ _____ by visiting

Permanent / Communication address of the customer as available on bank record. Following details are found in the verification of customer

Date of Account Opening	
Present Account Status	Operative / Inoperative / Closed / Unclaimed
Mode of Operation	
Name of the person to whom met	
Relationship with the customer	Self / other _____
Turn over in last 6 months	Total Amount – Dr. – Rs. _____ Lakh Total Amount – Cr. – Rs. _____ Lakh
Average Balance Maintained in the account for last SIX months	Rs. _____ Lakh
Nature of Transactions	i) Cash Deposit followed by immediate outward remittance ii) Inward remittance followed by immediate cash withdrawals iii) Single Credit Multiple Debit iv) Multiple Credit Single Debit v) High number of UPI transactions of small value vi) Any other suspicious pattern of transactions
Reason for such exceptional transactions in the account	

	Yes	No	Not Traceable
Whether address found correct?			
Whether address of the customer is easy to locate?			
Whether source of income is in line with the transactions in the account?			
Whether business transactions are routed through Saving account?			
Any suspicious activity found?			
Are income documents being available?			
Overall Comments			

Long Form:

AML: Anti Money Laundering
KYC: Know Your Customer
FIU-IND: Financial Intelligence Unit of India

CDD: Customer Due Diligence
EDD: Enhanced Due Diligence
CAP: Customer Acceptance Policy
CIP: Customer Identification Procedure
UCIC: Unique Customer Identification Code
BO: Beneficial Owner
CCR: Counterfeit Currency Report
CTR: Cash Transaction Report
STR: Suspicious Transaction Report
NTR: Non-Profit Organization Transaction Report
FATF: Financial Action Task Force

IT is reviewed and addition of following points.

- Monitoring of Transactions:-
- Customer Risk Rating Policy
- Ongoing due diligence
- Secrecy obligation and sharing information
- AML Rules (STR rules)
- OTP based e-KYC
- V-CIP

Chief Executive Officer.