



Rajkot Peoples Co-Operative Bank Limited

KYC POLICY

For F.Y. 2025-2026

Version: 1.11

RBI Master Direction		
RBI Circular Ref. No.	Date	Particulars
RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14. 01.001/2015-16	last updated as on 06.11.2024	

APPROVED BY BOD				
Version No.	By Resolution Date	By Resolution No	Purpose Review/ Modification	Reviewer/Approver
1.11	29.03.2025	30	Review	Board

Table of Contents

0	Key Data
1	Introduction
2	Purpose and objectives
3	Scope and application of KYC Policy of the Bank
4	Preliminary
5	Definitions
6	General
7	Purpose
8	Objective
9	Monitoring of Transactions
10	Money Laundering and Terrorist Financing Risk assessment by the bank
11	Designated Director
12	Principal Officer
13	Compliance of KYC policy
14	Customer Acceptance Policy
15	Risk Management
16	Customer Identification Procedure (CIP)
17	Customer due Diligence Procedure(CDD)
18	Record Management
19	Reposting requirements to Financial Intelligence Unit- India
20	Requirements/obligations under international Agreements –Communications from international Agencies
21	Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):
22	Other instructions
23	CDD Procedure and sharing KYC information with Central KYC records registry (CKYCR)
24	Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):
25	Period of presenting payment instruments
26	Operation of bank accounts and money mules
27	Collection of account payee cheques
28	Introduction of New Technologies (Debit cards/Mobile Banking/RTGS/ECS/IMPS etc.)
29	Correspondent Banking
30	Wire Transfer
31	Issue and payment of Demand Drafts etc.
32	Quoting of PAN
33	Selling third party products
34	At par cheque facility availed by co-operative banks
35	Issuance of prepaid payment instruments (PPIs)
36	Hiring of employees and employee training
37	Authority and control of policy
38	Review of policy
39	Disclosure of policy
40	Performance Reporting
41	Approval by Board of Directors

Key Data

❖ Document control

Document Title:	KYC Policy
Document ID:	KYCP
Document Version:	1.11
Effective Date:	01.04.2025

❖ Document Publication History

Document Author:	CS Juli Gadhiya
Document Prepared by:	CS Juli Gadhiya
Document Reviewed by:	MD & CEO
Document Approved by:	Board
Initial Release version:	1.0
Initial Released date:	31.01.2022

❖ Document Revision History

<i>Version</i>	<i>Board Meeting date</i>	<i>Board Resolution no</i>	<i>Change author</i>	<i>Change approver</i>	<i>Purpose</i>
1.11	29.03.2025	30			Review
1.10	18.06.2024	12			Review
1.9	15.03.2024	13			Modification
1.8	22.01.2024	18			Review
1.7	21.11.2023	12			Modification
1.6	21.07.2023	20			Review
1.5	30.05.2023	21			Modification
1.4	29.04.2023	19			Review
1.3	14.12.2022	14			Review
1.2	15.07.2022	14			Review
1.1	13.04.2022	21			Review
1.0	31.01.2022	10			Review

❖ Document Distribution List

No.	Name	Organization/Department	Purpose
1			

Rajkot Peoples Co-operative Bank Limited

Know Your Customer(KYC) Policy

1 Introduction

1. In terms of the provisions of Prevention of Money- Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India and other Laws / regulations, Bank is required to follow certain customer identification procedure while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions.
- 2 This KYC Policy is issued as per RBI's Master Direction on Know Your Customer (updated up to 06.11.2024).

2 Purpose and Objectives

- 1 India, being a member of Financial Action Task Force (FATF) is committed to upholding measures to protect the integrity of international financial system. To prevent Bank from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of various rules and regulations. The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:
- 2 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.
- 3 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.
- 4 The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in

terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

- 5 For this Policy, the term 'Money Laundering' would also cover financial transactions where the end use of funds is for financing terrorism, irrespective of the source of funds.

3 Scope and applicability of KYC Policy of the Bank

- 1 All offices of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time.
- 2 The provisions of KYC Policy guidelines shall apply to all the branches / offices of the Bank. Provided this rule shall not apply to 'small accounts'.
- 3 RBI vide MD dated 17.10.23 instructed Bank that where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India. RBI may advise further necessary action by the Bank including application of additional measures to be taken by the Bank to manage the ML/TF risks.

4 Preliminary

1 Short Title

Policy guidelines on Know Your Customer (KYC) Norms / Anti Money laundering (AML) Standards / Combating of Financing of terrorism (CFT) Measures / Obligation of the Bank under Prevention of Money Laundering Act (PMLA), 2002 shall be called as Know Your Customer (KYC) Policy, 2025.

5 Definitions

In terms of RBI's Master Directions on KYC last updated, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them as below:

Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

- 5.1 **“Aadhaar number”** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
- 5.2 **“Act” and “Rules”** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
- 5.3 **“Authentication”**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- 5.4 **Beneficial Owner (BO)**
- 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.
Explanation- For the purpose of this sub-clause-
1. **“Controlling ownership interest”** means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
2. **“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.

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.
- 5.5 **“Certified Copy”** - Obtaining a certified copy by the Bank shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the branch under his authorized number. Branch Official will also attest the duly signed photograph of the customer.
- 5.6 **“Central KYC Records Registry” (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- 5.7 **“Designated Director”** means a person designated by the bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include a person who holds the position of senior management or equivalent designated as a 'Designated Director'. Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.
- 5.8 **“Digital KYC”** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the branch of the bank as per the provisions contained in the Act.
- 5.9 **“Digital Signature”** shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- 5.10 **“Equivalent e-document”** means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

- 5.11 “Group”** – The term “group” shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).
- 5.12 “Know Your Client (KYC) Identifier”** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- 5.13 “Non-profit organisations” (NPO)** means any entity or organization, 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).
- 5.14 “Officially Valid Document” (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

- a. **in case of updated address**, where the customer submits his/her proof of possession of Aadhaar number as an OVD, he/she may submit it in such form as are issued by the Unique Identification Authority of India and/or
- b. **where the OVD furnished by the customer does not have updated address**, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

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

Further, at the time of on-boarding of the customer, an undertaking should be obtained from the customer along with AOF/OVDs stating that Customer shall submit his OVD with updated current address within 3 months failing which operations in his account shall be restricted.

- c. the customer shall submit OVD with current address within a period of 3 months of submitting the documents specified at 'b' above, failing which the operations in the account shall be restricted (Debit-frozen).
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

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

5.16 “Person” has the same meaning as assigned in the Act and includes:

- a. an individual,
- b. a Hindu undivided family,
- c. a company,
- d. a firm,
- e. an association of persons or a body of individuals, whether incorporated or not,
- f. every artificial juridical person, not falling within any one of the above persons (a to e), and
- g. any agency, office or branch owned or controlled by any of the above persons (a to f).

5.17 “Principal Officer” means an officer at the management level nominated by the bank, responsible for furnishing information as per rule 8 of the Rules.

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

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

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

5.19 ‘**Small Account**’ means a savings account which is opened in terms of sub rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in relevant section.

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

- a. opening of an account;
- b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- c. the use of a safety deposit box or any other form of safe deposit;
- d. entering into any fiduciary relationship;
- e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
- f. establishing or creating a legal person or legal arrangement.

Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

5.21 “**Common Reporting Standards**” (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

5.22 “**Customer**” means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

- 5.23** “Walk-in Customer” means a person who does not have an account-based relationship with the bank, but undertakes transactions with the bank.
- 5.24** “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification. 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 50,000/-, 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.
- 5.25** “Customer identification” means undertaking the process of CDD.
- 5.26** “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- 5.27** “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the bank.
- 5.28** “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that those are consistent with Banks’ knowledge about the customers, customers’ business and risk profile, the source of funds / wealth.
- 5.29** Payable-through accounts: The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

- 5.30** “**Periodic Updation**” means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- 5.31** “**Shell Bank**” means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
- 5.32** “**Video based Customer Identification Process (V-CIP)**”: an alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the bank by undertaking seamless, secure, live, informed consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.
- 5.33** “**Wire transfer**” related definitions:
- a. **Batch transfer:** Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.
 - b. **Beneficiary:** Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
 - c. **Beneficiary bank:** It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary bank and makes the funds available to the beneficiary.
 - d. **Cover Payment:** Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
 - e. **Cross-border wire transfer:** Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
 - f. **Domestic wire transfer:** Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary

financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.

- g. Financial Institution:** In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
- h. Intermediary Bank:** Intermediary bank refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
- i. Ordering Bank:** Ordering bank refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
- J. Originator:** Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
- k. Serial Payment:** Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).
- l. Straight-through Processing:** Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.
- m. Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
- n. Wire transfer:** Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6 General

- 1 RBI has advised the Bank that a Know Your Customer (KYC) Policy, duly approved by the ACB/ Board of Directors of the Bank, be formulated and put in place.
- 2 Further, this policy framework should seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks.

7 Purpose

- 1 The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.
- 2 For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

8 Objective

- 1 The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:
 - a. 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.

- c. 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
- d. To cooperate with various government bodies dealing with related issues.

The KYC policy shall include following four key elements:

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

9 Monitoring Of Transactions

- 1 Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds. Bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI and ML) to support effective monitoring.

10. Money Laundering and Terrorist Financing Risk Assessment by the bank:

- 1 The bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. 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.
- 2 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 the bank. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the bank to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it **should be reviewed at least annually**.
- 3 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.

- 4 Bank may apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and may have Board approved policies, controls and procedures in this regard. Bank will implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, bank shall monitor the implementation of the controls and enhance them if necessary.
- 5 Audit Department shall carry out the above said Risk Assessment review of branches at least on annual basis. The outcome of the exercise shall be put up to the ACB of the Board and should be available to competent authorities. Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have approve controls and procedures in this regard. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

11 Designated Director

- 1 A Director on the Board to be nominated as “Designated Director”, as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
- 2 Designated Director shall be nominated by the Board.
- 3 The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
- 4 In addition to communicating to the FIU-IND, The Bank shall communicate the name, designation address and contact details of designated director and principal Officer to the Reserve Bank also.
- 5 In no case, the Principal Officer be nominated as the 'Designated Director'.

12 Principal Officer

- 1 The Board will nominate competent officer as Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations.

- 2 The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- 3 Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.
- 4 **The Principal Officer will report to audit department who shall be the administrative head of Audit department. The Principal Officer will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.**

13 Compliance of KYC policy

- 1 Compliance with KYC Policy is to be ensured through:
 - 1 All HO Divisions to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
 - 2 Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Compliance Division, HO.
 - 3 **Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.**
 - 4 Concurrent / internal audit to also ensure verification of compliance with KYC guidelines.
- 2 It is to be ensured that decision-making functions of determining compliance with KYC norms are not outsourced by the bank.
- 3 PML Rules require all offices of the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment should- be documented;

- i. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
 - ii. be kept up to date; and
 - iii. be available to competent authorities and self-regulating bodies.
 - iv. Bank shall treat the risk categorization and reasons for risk categorization of customers as confidential.
- 4 The implementation of KYC-AML guidelines by branches in letter and spirit, has to be ensured by Head Office and the same is to be checked during their visit to branches by H.O. Officials.

14 Customer Acceptance Policy

A Customer Acceptance Policy has been framed by the bank, as under without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, it is to be ensured that:

1. No account is opened in anonymous or fictitious/benami name.
2. No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The RE shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
3. No transaction or account-based relationship is undertaken without following the CDD procedure.
4. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
5. Additional information, where such information requirement has not been specified in the internal KYC Policy of the RE, is obtained with the explicit consent of the customer.
6. Bank shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account or avail any other product or service from the same RE, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
7. CDD Procedure is followed for all the joint account holders, while opening a joint account.

8. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
9. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of this MD.
10. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
11. Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
12. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

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

Where a suspicion of money laundering or terrorist financing is formed, and it reasonably believed that performing the CDD process will tip-off the customer, CDD process shall not be pursued instead it shall be reported to HO for onward submission / file an STR with FIU-IND.

15. Risk Management

For Risk Management, The Bank may have a following risk-based approach which includes:

- 1 Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Bank.
- 2 Broad principles may be laid down by the bank for risk-categorization of customers.
- 3 Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, etc. While considering customer's identity, the ability to confirm identity documents through

online or other services offered by issuing authorities may also be factored in. It is hereby specified that the various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

- 4 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.

Explanation: FATF Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

16 Customer Identification Procedure (CIP)

Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:

- 1 Commencement of an account-based relationship with the customer.
- 2 When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
- 3 Selling third party products as agents, selling their own products, and any other product for more than rupees fifty thousand.
- 4 Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
- 5 When a bank has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- 6 REs shall ensure that introduction is not to be sought while opening accounts.
- 7 For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements in line with the requirements and obligations under the PML Act. And undertaking enhanced due diligence measures, as applicable, will be with the Bank.

17 Customer due Diligence (CDD) Procedure

1 Customer Due Diligence (CDD) Procedure in case of Individuals

1 For undertaking CDD, concerned offices shall obtain the following from an individual 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:

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

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

(ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

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

(c) 1 recent photograph; and such other documents including in respect of the nature of business and financial status of the customer, Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

ii) Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the bank.

iii) Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.

iv) an equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Bank shall carry out verification through digital KYC as specified under Annex I of RBI master guidelines on KYC.

v) KYC Identifier under clause (ac) above, the Bank shall retrieve the KYC records online from the CKYCR in accordance with relevant section in this regard.

Provided further that in case e-KYC authentication (OTP on mobile linked authentication) cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank.

2 The database shall be subjected to periodic internal audit/inspection by the bank and shall be available for supervisory review.

3 The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

Explanation 1: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 2: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

- 4 While establishing an account based relationship with individual customer, the branch official to ascertain as to whether the customer is already having a Customer ID with the Bank. In case the customer has an existing Customer ID, fresh Customer ID shall not be created and the new account shall be opened with the existing Customer ID.
- 5 The name, father's name, date of birth and address of the customer be filled in the same manner and style as it appears in the PAN Card / KYC document provided by the customer. Branch official will ensure that all the mandatory fields in Account Opening Form / Customer Master Form such as Name, Fathers' name, date of birth, address, Identity Proof, address proof, Identification number (Identity proof document number), Profession / activity (Nature of Business - specific), total annual income, total annual turnover (in case of business) etc. are completely and correctly filled in by the customer and are also correctly captured in customer's database in CBS. The respective _____ deaprtments of the bank shall ensure that a c c o unts are capturing correct data in CBS system, particularly in respect of Constitution Code, Profession/ Activity, Occupation, Income/ Turnover etc. as risk category of the customer is assigned on the basis of these parameters.
- 6 In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain. PAN Card and Voter Identity Card, wherever obtained, be verified on-line through the following websites and a print of on-line verification of the said document be held on record with the relevant AOF:

Name of Documents	Website / link
PAN CARD	On line pan verification
VOTERS' ID card	www.nvsp.in (national voters service portal)

As a matter of policy in our Bank, Accounts in non-face to face mode will not to be opened using Aadhaar OTP based e-KYC and Video based Customer Identification Process (V-CIP) till creation of required infrastructure and skill up gradation of staff.

2 CDD Measures for Sole Proprietary firms

- 1 For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

- 2** In addition to the above, any two of the following documents or the equivalent e-documents thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

a	Registration certificate including Udyam Registration Certificate (URC) issued by the Government
b	Certificate/licence issued by the municipal authorities under Shop and Establishment Act
c	Sales and income tax returns
d	CST/VAT/ GST certificate
e	Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
f	IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute
g	Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities
h	Utility bills such as electricity, water, landline telephone bills, etc.

- 3** In cases where the bank is satisfied that it is not possible to furnish two such documents, bank may, at its discretion, accept only one of those documents as proof of business/activity. Provided REs undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

3 CDD Measures for Legal Entities:

1	For opening an account of a Company, [certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:]
1.1	Certificate of incorporation
1.2	Memorandum and Articles of Association
1.3	Permanent Account Number of the company
1.4	A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
1.5	Documents, as specified in CDD Procedure of individuals, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

1.6	the names of the relevant persons holding senior management position; and
1.7	the registered office and the principal place of its business, if it is different.
1.8	If any, as may be decided by the bank from time to time.

2	For opening an account of a Partnership firm, [the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:]
2.1	Registration certificate
2.2	Partnership deed
2.3	Permanent Account Number of the partnership firm
2.4	Documents, as specified in CDD procedure of individuals relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
2.5	the names of all the partners and
2.6	address of the registered office, and the principal place of its business, if it is different.
2.7	If any, as may be decided by the bank from time to time.

3	For opening an account of a Trust, [certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:]
3.1	Registration certificate
3.2	Trust deed
3.3	Permanent Account Number or Form No.60 of the trust
3.4	Documents, as specified in CDD procedure of individuals relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
3.5	the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
3.6	the address of the registered office of the trust;
3.7	list of trustees and documents under CDD procedure of individuals relating to beneficial owner, for those discharging role as trustee and authorised to transact on behalf of the trust.
3.8	If any, as may be decided by the bank from time to time.

4	For opening an account of an unincorporated association or a body of individuals, [certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:]
---	---

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

4.1	Resolution of the managing body of such association or body of individuals
4.2	Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
4.3	Power of attorney granted to transact on its behalf
4.4	Documents, as specified in paragraph 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
4.5	Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.
4.6	If any, as may be decided by the bank from time to time.
	Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.
5	For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, [certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified]
5.1	Document showing name of the person authorised to act on behalf of the entity
5.2	Documents, as specified in CDD Procedure of individuals of the person holding an attorney to transact on its behalf and
5.3	Such documents as may be required by the bank to establish the legal existence of such an entity/juridical person.
5.4	
5.5	Provided that in case of a trust, the bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses of 16.4 and 16.6 of customer identification procedure as mentioned above in this policy.
5.6	If any, as may be decided by the bank from time to time.
	Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.
6	For opening an account of Hindu Undivided Family, [certified copies of each of the following documents shall be obtained:]

6.1	Identification information as specified in CDD procedure of individuals of the person in respect of the Karta and Major Coparceners
6.2	Declaration of HUF and its Karta
6.3	Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
6.4	The Permanent Account Number document thereof or Form No. 60 as defined in Income-tax Rules, 1962.
6.5	If any, as may be decided by the bank from time to time.

4 Identification of Beneficial Owner

7	For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of subrule (3) of Rule 9 of the Rules to verify his/her identity shall be undertaken keeping in view the following:
7.1	Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
7.2	In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.
7.3	Provided that in case of a trust, the Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of Section 13 of MD of RBI dated 17.10.23.
7.4	If any, as may be decided by the bank from time to time.

5 On-going Due Diligence

- 1 on-going due diligence of customers to be undertaken to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
- 2 Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

- (a) Large and complex transactions including RTGS 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.
- (d) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
- (f) For ongoing due diligence, REs may consider adopting appropriate software technology/technologies to support effective monitoring.

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

- (a) A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

- (b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.
Explanation: High risk accounts have to be subjected to more intensified monitoring.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

4 Updation / Periodic Updation of KYC

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.

A risk-based approach is adopted by the Bank for periodic updation of KYC.

High Risk Customers	
I	However, periodic updation shall be carried out at least once in every two years for high-risk customers.
Medium Risk Customers	
II	Once in every eight years for medium risk customers
Low Risk Customers	

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

III	Once in every ten years for low-risk customers from the date of opening of the account / last KYC updation.
The detailed 'Standard Operating Procedure for Periodic KYC Updation' has been placed at Annexure.	

4.1	Individuals
i	No change in KYC information
	In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Bank, customer's mobile number registered with the bank, ATMs, digital channels (such as mobile application) letter, etc.
ii)	Change in address
	In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as mobile application), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.
iii)	Accounts of customers, who were minor at the time of opening account, on their becoming major:
	In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the base branch. Wherever required, branch may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major. As the KYC documents are to be maintained at base branch, the customer may contact his/her base branch.

4.2	Customers other than individuals
i	No change in KYC information
	In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the bank, ATMs, digital channels (such as mobile application), letter from an official authorized by the LE in this regard, board resolution, etc. Further, bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

	and shall update the same, if required, to keep it as up-to-date as possible.
ii)	Change in KYC information
	In case of change in KYC information, RE shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.
4.3	Additional measures
	No change in KYC information
	In addition to the above, it shall ensure by the concerned office that,
I	The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the bank 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, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
II	Customer's PAN details, if available with the bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.
III	Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation/ periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/ periodic updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
IV	In order to ensure customer convenience, bank may consider making available the facility of updation/ periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board.
V	In case of existing business relationship which is not KYC compliant, operations in the account to be temporarily ceased. However, before temporarily ceasing operations for an account, it is to be ensured to give the client two notices of 30 days each and within 30 days period the account should be made KYC compliant otherwise operations in the account shall be frozen. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

VI	Bank may advise the customers that in order to comply with the PML rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.
VII	Bank shall adopt a risk-based approach with respect to periodic updation of KYC. And as a part of Risk based approach, the bank will mandate as an additional and exceptional measures such as: while updation of KYC information requirement of obtaining recent photograph, requirement of physical presence of the customer, and a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be done by the bank.
4.4	Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship/ account-based relationship and thereafter, as necessary; customers shall submit to the bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at bank's end.
5	In case of existing customers, bank shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date as may be notified by the Central Government, failing which bank shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.
	Explanation – For the purpose of this paragraph, “temporary ceasing of operations” in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the bank till such time the customer complies with the provisions of this paragraph. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.
	Provided that before temporarily ceasing operations for an account, the bank shall give the customer an accessible notice and a reasonable opportunity to be heard .

	Further, bank may give appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.
	Provided further that if a customer having an existing account-based relationship with the bank gives in writing to the bank that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, the bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

6 Enhanced and Simplified Due Diligence Procedure

1	Enhanced Due Diligence for High Risk Customers
1.1	In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Branches shall take a robust process of due diligence for dealing with requests for change of registered mobile number.
1.2	Apart from obtaining the current address proof, concerned official shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
1.3	PAN shall be obtained from the customer and it shall be verified from the verification facility of the issuing authority.
1.4	First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
2	Accounts of Politically Exposed Persons (PEPs) Bank shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:
2.1	Bank have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
2.2	Reasonable measures are taken by the bank for establishing the source of funds / wealth

2.3	the approval to open an account for a PEP shall be obtained from the senior management;
2.4	all such accounts are subjected to enhanced monitoring on an on-going basis;
2.5	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;
2.6	These instructions shall also be applicable to family members or close associates of PEPs. Explanation: For the purpose of this paragraph, "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.

3	Simplified Due Diligence
	Simplified norms for Self Help Groups (SHGs)
3.1	CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
3.2	CDD of all the office bearers shall suffice.
3.3	CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs.

18 Record Management

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

1. maintain all necessary records of transactions between the bank and the customer, both domestic and international, for at least five years from the date of transaction;
2. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
3. make available swiftly, the identification records and transaction data to the competent authorities upon request;
4. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

5. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
 - (i) the nature of the transactions;
 - (ii) the amount of the transaction and the currency in which it was denominated;
 - (iii) the date on which the transaction was conducted; and
 - (iv) the parties to the transaction.
6. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
7. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.
 - i. Explanation. – For the purpose of this paragraph, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.
8. 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.

19 Reporting Requirements to Financial Intelligence Unit – India

- 1 **Bank/The BO/Head Office** shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of rule 7 thereof.
- 2 The following reports shall be furnished to Financial Intelligence Unit-India as per guidelines prescribed by RBI / FIU as applicable and within the timelines specified.

Reports to be furnished to Financial Intelligence Unit – India

 - (i) Cash Transaction Report [CTR].
 - (ii) Suspicious Transactions Report [STR]
 - (iii) Counterfeit Currency Report [CCR]
 - (iv) Non Profit Organizations Transaction report [NTR]

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

1	Cash Transaction Report (CTR)
I	Report of all cash transactions of the value of more than Rs. 10 Lakhs (rupee ten lakhs) or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh.
II	The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.
2	Suspicious Transaction Reports (STR)
I	While determining suspicious transactions, bank is to be guided by the definition of “suspicious transaction” as contained in PMLA Rules as amended from time to time.
	"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
a.	gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b.	appears to be made in circumstances of unusual or unjustified complexity; or
c.	appears to not have economic rationale or bona-fide purpose; or
d.	Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism. Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.
(ii)	It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted transactions in STRs to be reported, even if not completed by the customers, irrespective of the amount of the transaction.
(iii)	STR to be submitted 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.
(iv)	Furnishing of STR to be ensured within seven days of arriving at a conclusion by the Principal Officer and committee of General Managers of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

Rajkot Peoples Co-Operative Bank Ltd
KYC Policy - 2025-2026

(v)	It shall be ensured 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
(vi)	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. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular. For effective monitoring of transactions of the customers, Bank has implemented an AML system of the bank software for generation of AML alerts on the pre-defined scenarios, as advised by Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. In case any suspicious transaction is detected, the same be reported to Committee of General Managers by Principal Officer for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FINnet Gateway after getting the approval of GM Committee.
	Indicative list of various types of indicators i.e. customer behaviour and risk based transaction monitoring, high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at Annexure.
3	Counterfeit Currency Report (CCR) Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.
4	Non Profit Organizations Transaction report [NTR] All transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency, to be reported to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.
5	Cross-border Wire Transfer Report [CWTR] Cross-Border Wire Transfer Report (CWTR) to be filed to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

- 3 While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts merely on the basis of the STR filed.
- 4 Bank's directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under relevant section of RBI KYC Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.
- 5 Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

20 Requirements/obligations under International Agreements - Communications from International Agencies

- 1 Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:
 - (a) **All branches of the Bank** shall ensure that in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:
 - i. The "ISIL (Da'esh) & Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the AlQaida is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
 - ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at <https://www.un.org/securitycouncil/sanctions/1988/materias>.

- 2 All branches of the Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the bank for meticulous compliance.
- 3 Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 (Annex II of RBI Master Direction on KYC).
- 4 Freezing of Assets under section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of this Master Direction), shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

21 Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

- 1 All offices of the bank shall ensure meticulous compliance with the “Procedure for Implementation of section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annex III of RBI Master Direction on KYC).
- 2 In accordance with paragraph 3 of the aforementioned Order, All offices of the bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
- 3 Further, all offices of the bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

- 4 In case of match in the above cases, REs shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.
- 5 The offices of the bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- 6 In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, 2005, Bank shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
- 7 In case an order to freeze assets under section 12A is received by the bank from the CNO, bank shall, without delay, take necessary action to comply with the Order.
- 8 The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.
- 9 Bank shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementationof-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.
- 10 In addition to the above, Bank shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.

- 11 Bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organization of which India is a member and accepted by the Central Government.

22 Other Instructions

1 Secrecy Obligations and Sharing of Information:

- 1 All offices of the bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the bank and customer.
- 2 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.
- 3 While considering the requests for data/information from Government and other agencies, all offices of the 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 transactions.
- 4 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. Where the interest of bank requires disclosure, and
 - iv. Where the disclosure is made with the express or implied consent of the customer.

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

- 1 Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- 2 In terms of provision of Rule 9(1A) of the PML Rules, the bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- 3 Operational Guidelines for uploading the KYC data have been released by CERSAI.

- 4 The bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- 5 Bank shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the LE Template released by CERSAI.
- 6 Once KYC Identifier is generated by CKYCR, REs shall ensure that the same is communicated to the individual/LE as the case may be.
- 7 In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the concerned offices of the bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates respectively, at the time of periodic updation as specified in kyc policy, or earlier, when the updated KYC information is obtained/received from the customer.
- 8 Also, whenever the RE obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, 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 shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs to the bank regarding an update in the KYC record of an existing customer, the bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the bank.
- 9 Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
- 10 For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall

not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

- (i) there is a change in the information of the customer as existing in the records of CKYCR; or
- (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
- (iii) the validity period of downloaded documents has lapsed; or
- (iv) the offices of the bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

24 Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

- 1 Under FATCA and CRS, all offices of the bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F.

25 Period for presenting payment instruments

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

26 Operation of Bank Accounts & Money Mules

- 1 The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the concerned bank, it shall then be deemed that the bank has not complied with these directions.

27 Collection of Account Payee Cheques

- 1 Account payee cheques for any person other than the payee constituent shall not be collected.

- 2 Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by bank.
- 3 The bank shall, at their option, not issue UCIC to all walk- in/occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

28 Introduction of New Technologies (Debit cards/Mobile Banking/RTGS/ECS/IMPS etc.

- 1 Bank shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and preexisting products.
- 2 Further, bank shall ensure:
 - (a) Adequate attention shall be paid by Bank to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products / services / technologies. ; And
 - (b) Adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD (Enhanced due diligence) measures and transaction monitoring, etc.

29 Correspondent Banking

- 1 Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). These services include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks shall use the publicly available information which, inter alia, should include
 - (a) Information relating to the reputation of the respondent institution
 - (b) The quality of supervision in the concerned jurisdiction
 - (c) Whether the respondent institution has been subjected to any investigation or regulatory action relating to Money Laundering / Terrorist Financing.
- 2 Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent banking and other similar

relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

- 3 Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.
- 4 The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.
- 5 Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.
- 6 Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.
- 7 In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts of the correspondent bank and is undertaking on-going 'due diligence' on them.
- 8 The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.
- 9 Correspondent relationship shall not be entered into or continued with a shell bank. (i.e. a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).
- 10 It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.
 - 11 Banks shall be cautious of correspondent banking relationships with institutions located in jurisdictions which have strategic

deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

- 12 Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

30 Wire Transfer

A. Information requirements for wire transfers:

- 1 All offices shall ensure the following while effecting wire transfer:
- 1 All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below: a. name of the originator;
 - 2 the originator account number where such an account is used to process the transaction;
 - 3 the originator's address, or national identity number, or customer identification number, or date and place of birth;
 - 4 name of the beneficiary; and
 - 5 the beneficiary account number where such an account is used to process the transaction.
- 2 In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.
- 3 In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.
- 4 Domestic wire transfer, where the originator is an account holder of the ordering bank, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.
- 5 Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

- 6 In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering bank and where the information accompanying the wire transfer can be made available to the beneficiary bank and appropriate authorities by other means, it is sufficient for the ordering bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering bank shall make the information available within three working/business days of receiving the request from the intermediary bank, beneficiary bank, or from appropriate competent authorities.
- 7 All offices shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting / competent authorities as well as FIU-IND on receiving such requests with appropriate level provisions.
- 8 The wire transfer instructions are not intended to cover the following types of payments:
 1. Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.
 2. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the obligation of a bank to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

B. Responsibilities of ordering RE, intermediary RE and beneficiary RE, effecting wire transfer, are as under:

9 Ordering Bank

- 1 The ordering bank shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.
2. Customer Identification shall be made if a customer, who is not an account holder of the ordering bank, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.
3. Ordering bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this paragraph

10 Intermediary Bank

- 1 Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.
- 2 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary bank.
- 3 Intermediary bank shall take reasonable measures to identify cross border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing
- 4 Intermediary bank shall have effective risk-based policies and procedures for determining:
 - (a) When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
 - (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

11 Beneficiary Bank

- 1 Beneficiary bank shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.

- 2 Beneficiary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.
- 12 **Money Transfer Service Scheme (MTSS) providers and other REs,** are required to comply with all of the relevant requirements of this paragraph, whether they are providing services directly or through their agents. Bank that control both the ordering and the beneficiary side of a wire transfer shall: a. take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and b. file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.
- 13 **Other Obligations**
- 1 **Obligations in respect of REs' engagement or involvement with unregulated entities in the process of wire transfer:** Bank shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,
- A there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
- B the agreement / arrangement, if any, with such unregulated entities by REs clearly stipulates the obligations under wire transfer instructions; and
- C a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

14 Bank's responsibility to fulfil record management requirements complete originator and beneficiary information relating to wire transfers shall be preserved by the bank involved in the wire transfer, in accordance with Master Direction on KYC.

31 Issue and Payment of Demand Drafts, etc.

1 Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment. Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

32 Quoting of PAN

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

33 Selling Third party products

1 REs acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

- (a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 13(e) of this Direction.
- (b) Transaction details of sale of third-party products and related records shall be maintained as prescribed in paragraph 46 of Chapter VII.
- (c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
- (d) Transactions involving rupees fifty thousand and above shall be undertaken only by:
 - 1 debit to customers' account or against cheques; and
 - 2 obtaining and verifying the PAN given by the account-based as well as walk-in customers.
- (e) Instruction at 'd' above shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of

prepaid/travel cards and any other product for rupees fifty thousand and above.

34 At-par cheque facility availed by co-operative banks

- 1 The 'at par' cheque facility offered by co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.
- 2 The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by banks.
- 3 Bank shall:
 - i. ensure that the 'at par' cheque facility is utilised only:
 - a. for their own use,
 - b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
 - c. for walk-in customers against cash for less than rupees fifty thousand per individual.
 - ii. maintain the following: a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque, b. sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.
 - iii. Ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

35 Issuance of Prepaid Payment Instruments (PPIs)

- 1 PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

36 Hiring of Employees and Employee training

- 1 Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
- 2 bank shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing

KYC/AML/CFT landscape, nationally and internationally. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

- 3 On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the RE, regulation and related issues shall be ensured.

37 Review and amendment of the Policy

- 1 The Board will review the policy. The policy will be scheduled for a comprehensive review on or before March 31, of every year or as and when deem necessary by the Board.
- 2 This Policy shall be reviewed at least annually or earlier, as and when needed, if required due to regulatory changes by Board.
- 3 This review will be initiated by the Compliance Department of the Bank and conducted by the concerned officers of the Bank.
- 4 Amendments, if any, shall be made to keep it align with changes, if any in RBI guidelines and regulations and shall require Board approval.

38 Control of the Policy

- 1 Compliance team will develop & implement procedures for the benchmarking & evaluation performance of this policy to meet the objective as stated within this the policy.
- 2 Compliance with this policy will be monitored by the Compliance Department of the Bank. Levels of compliance will be reported periodically to CEO of the Bank.

39 Performance Reporting

- 1 The Board of Directors of the bank shall review performance of this policy and compliance with policy minimum **once in a financial year or as and when felt necessary.**

40 Approval by Board of Directors/Adoption Clause

- 1 This KYC Policy was approved and adopted by the Board of Directors of Rajkot Peoples Co-Operative Bank Limited at its duly convened