Policy of Know Your Customer (KYC), Anti Money Laundering (AML) and Combating Financing Terrorism (CFT) of Erode District Central Cooperative Bank Ltd.,

1. INTRODUCTION:

1.1 The Bank has in place a Policy on KNOW YOUR CUSTOMER (KYC) norms, ANTI MONEY LAUNDERING (AML) and Combating Financing Terrorism (CFT) measures approved by the Board of Directors. The policy was based on the then prevailing guidelines issued by RBI.

1.2 The KYC guidelines have regularly been revisited by RBI in the context of the recommendations made by the Financial Action Task Force (FATF) and PMLA on AML standards and on CFT. These guidelines advise Banks to follow certain Customer Identification Procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority.

1.3 This policy has been complied taking into account cognizance of the guidelines enumerated in the Master Direction of RBI in RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No. 81/14.01.001/015-16 dated 25.02.2016 (updated as on May 04, 2023).

2. OBJECTIVES OF THE POLICY:

2.1 To comply with the guidelines prescribed by Reserve Bank of India on KYC norms, AML measures and Combating Financing Terrorism(CFT) based on the recommendations of the Financial Action Task Force (FATF) and provisions under PMLA.

2.2 To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities.

2.3 To enable the Bank to know/understand its customers and their financial dealings better, which in turn would help it to manage its risks prudently.

2.4 To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures and regulatory guidelines.

2.5 To ensure that the dealing staff is adequately trained in KYC/AML/CFT procedures.

3. SCOPE OF THE POLICY:

3.1 The Policy is applicable across all branches of the Bank and it is to be read in conjunction with related operational guidelines issued from time to time.

3.2 The contents of the policy shall always be read in tandem/autocorrected with the changes/modifications which may be advised by RBI and/or by PMLA and its amendments/or by any regulators and/or by Bank from time to time.

4. DEFINITIONS AND EXPLANATION OF VARIOUS TERMS:

4.1 For the purpose of KYC, a 'Customer' is defined as:

4.1.1 A person or entity that maintains an account and/or has a business relationship with the Bank.

4.1.2 One on whose behalf the account is maintained (ie. a Beneficial Owner)

4.1.3 Beneficiaries of transactions conducted by professional intermediaries, that acts on behalf of its customers to conduct a transaction or open an account with the Bank. As per RBI, the term Financial Intermediary includes the following persons or entities registered under Section 12 of the Securities and Exchange Board of India Act 1992:

- Stock Brokers
- Merchant Bankers
- Sub-Brokers
- Underwriters
- Portfolio Managers
- Share Transfer Agents
- Depositories and Participants
- Bankers to an issue
- Custodian of Securities
- Trustees to Trust Deed
- Credit Rating Agencies
- Registers to Issue
- Venture Capital Funds
- Collective Investment Schemes including Mutual Funds

4.2 Beneficial Owner (BO):

4.2.1 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:

1. "Controlling Ownership Interest" means ownership of/entitlement to more than 25% 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.

4.2.2 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 15 per cent of capital or profits of the partnership.

4.2.3 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 per cent of the property or capital or profits of the unincorporated association or body of individuals.

4.2.4 Where the customer is a Trust, the identification of Beneficial Owner(s) shall include identification of the author of the Trust, the Trustees, the beneficiaries with 15% 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.

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

4.3.1 opening of an account
4.3.2 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'
4.3.3 the use of a safety deposit box or any other form of safe deposit'
4.3.4 entering into any fiduciary relationship;
4.3.5 any payment made or received, in whole or in part, for any contractual or other legal obligation; or
4.3.6 establishing or creating a legal person or legal arrangement.

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

4.4.1 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

4.4.2 appears to be made in circumstances of unusual or unjustified complexity; or

4.4.3 appears to not have economic rationale or bona-fide purpose; or
4.4.4 gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

4.5 "Officially Valid Document (OVD)" means the Passport, the Driving Licence, 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, letter issued by the National Population Register containing details of name and 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.

4.6 "Aadhar Number" as defined under Sub-Section (a) of Section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth 'The Aadhar Act', means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of demographic information and biometric information as per the provisions of the Aadhaar Act, 2016.

The Erode Dist. Central Co-op. Bank Ltd. E.T. HEAD OFFICE ERODE

4.7 "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.

4.8 "Authentication" as defined under sub-section (a) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

4.9 "Enrolment Number" means "Enrolment ID" as defined in Section 2(1)(j) of the Aadhaar (Enrolment and Update) Regulation, 2016 which means a 28 digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.

4.10 "E-KYC Authentication Facility" as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction.

4.11 "Identity Information", as defined in sub-section (n) of Section 2 of the Aadhaar Act, in respect of an individual, includes individual's Aadhaar number, biometric information and demographic information.

4.12 "Non-Profit Organisation (NPO)" means any entity or organisation 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.

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

aa. an individual
bb. a Hindu Undivided Family
cc. a Company
dd. a Firm
ee. an Association of Persons or a Body of Individuals, whether incorporated or not.
ff. Every artificial juridical person, not falling within any one of the above persons (aa to ee) and
gg. Any agency, office or branch owned or controlled by any of the above persons (aa to ff).

4.14 "Principal Officer" means an Officer nominated by the Bank, responsible for furnishing information as per Rule 8 of the Rules.

4.15 "Resident", as defined under sub-section (v) of Section 2 of the Aadhaar Act, means an individual, who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment for Aadhaar.

4.16 "Small Account" means a Savings account, in which:

4.16.1 the aggregate of all credits in a financial year does not exceed rupees one lakh.

4.16.2 The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand and

4.16.3 The balance at any point of time does not exceed rupees fifty thousand.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements

4.17 "Yes/No Authentication Facility" as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing "Yes" or "No", along with other technical details related to the authentication transaction, but no identity information.

4.18 "Branch" includes the Branches, Extension Counters and Sections at Head Office.

4.19 "Director" means a Director appointed under sub-section (1) of Section 49 of PML Act.

4.20 "Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rule 2 (ba) "Prevention of Money-Laundering (Maintenance of Records) Amendment Rules, 2013.

4.21 "Officer" means the person responsible for conducting the Branch or Sections at Head Office.

4.22 "High Net-Worth Individual" means an individual is considered a High Net-Worth Individual (HNI) for the purposes of the Bank if the sum of all the credits for the individual at the Bank in all products exceed Rs. 15 lakhs (Rs. 15,00,000)

4.23 "Politically Exposed Persons (PEPs)" means Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior executives of State-owned corporations, important political party officials, etc.

5. RESPONSIBILITIES:

5.1 Board of Directors

As per RBI guidelines, the Board of Directors of the Bank is responsible for ensuring that an effective KYC, AML and CFT programme is put in place by establishing procedures

and ensuring their effective implementation. The programme set by the Board of Directors shall contain:

a. Application procedures for AML measures developed by senior management;
b. Roles and responsibilities;
c. Training for bank officials;
d. Systems and controls for implementation;
e. Approving methodology for customer risk categorization; and
f. Management oversight for the KYC, AML and CFT programme.

It is the responsibility of the Board of Directors to appoint the Principal Officer (PO) and the Designated Director of the Bank for the purpose of ensuring KYC compliance.

All pertinent KYC, AML and CFT topics must be discussed by the Board of Directors in their quarterly meeting.

5.2 Designated Director

The Managing Director (a person who holds the position of senior management or equivalent designated as a 'Designated Director') shall be Designated Director will ensure the following function and compliance.

a. Implementation of KYC Norms, Combating of Financing of Terrorism (CFT), AML Standards, Prevention of Money Laundering (Amendment) Act, 2012 in our Bank.
b. To get access any of the information on customer data base, transactions, records etc. as instructed by RBI.
c. Maintaining liaison with law enforcement agencies, banks and other institutions.
d. Preservation of the records of transactions between the bank and the client.
e. Submission of periodical reports to the Board of Management, Financial Intelligence Unit of India and other regulatory agencies
f. Oversee the functioning of the Principal Officer.

5.3 Principal Officer

a. The Assistant General Manager(Banking) (indicate the designation of the Senior Officer who has been identified by the bank as Principal Officer here) shall be Principal Officer for KYC/AML/CFT matters who shall be responsible for implementation and compliance with the policy. His illustrative duties, in this regard, will be as follows: -

    i. Overall monitoring of the implementation of the Bank's KYC/AML/CFT policy.
    ii. Monitoring and reporting of transactions, and sharing of information, as required under the law.
    iii. Interaction with MLRO's (Money Laundering Reporting Officer) at the controlling offices for ensuring full compliance with the policy.
    iv. Timely submission of Cash Transaction Reports(CTRs), Suspicious Transaction Reports(STRs) and Counterfeit Currency Reports (CCRs) to FIU-IND
    v. Maintaining liaison with the law enforcement agencies, banks and other institutions, which are involved in the fight against money laundering and combating financing of terrorism.

vi. Ensuring submission of periodical reports to the Top Management/Board.

5.4 Senior Management

The Senior Management is responsible for the creation of policies and procedures and their responsibilities include but are not limited to:

a. Creation of KYC, AML and CFT policies subject to approval of the Board;

b. Deployment of suitable personnel and providing them with sufficient authority to ensure the effective implementation and administration of KYC, AML and CFT programmes;

c. Obtain periodic reports regarding transaction monitoring, KYC, AML and CFT initiatives, identified compliance deficiencies and corrective actions taken; and

d. Create updates or make changes to the existing policies and procedures which will be required to be ratified by the Board of Directors.

5.5 Branch Manager (BM)

The Branch Manager is the branch level decision making authority for ensuring implementation of all KYC & AML policy decisions. The responsibilities of the Officer include:

a. Responsibility for Implementation of KYC, AML and CFT policy at the Branch level;

b. Implementation of policy on closure or freezing of accounts for non-compliance;

c. Responsibility for submitting CTR / STR / CCR / NTR periodically or as and when required;

d. Escalation of transaction monitoring alerts from the branch level to the Bank level.

5.6 BM shall be the Account Opening Officer (AOO).

The Account Opening Officer owns the relationship with the customer and is responsible for:

a. Information review and approval for all new customers. While certain portions of the information collection process may be delegated to the Staff Assistant (SA), the Officer remains ultimately responsible;

b. Obtaining, maintaining and updating customer KYC information and documentation in the Bank's management systems;

c. Interacting with the customer or customer contact in order to make sure that the customer identification requirements are understood;

d. Forming a reasonable belief regarding the true identity of the customers; and

e. Performing periodic reviews of and accordingly refreshing customer's KYC information on file.

5.7 Staff

Bank staff who are interacting with customers and or handling customer transactions/instructions will be the Bank's strongest defence against money laundering. Hence, the communication of a Bank's KYC, AML and CFT Programme and the related training in how to apply the programme is key to the success of strategies related to Anti Money Laundering and Combating the Financing of Terrorism. It is also equally important for the staff to keep themselves updated with the policies and procedures related to their role in the organisation

Staff members of the Bank are also obligated to report transactions that are suspicious in nature and could be potentially money laundering or terrorist financing activity. An employee is required to report transaction activity based on mere suspicion even if he or she is not precisely sure about the underlying criminal activity or whether illegal activities have occurred.

6. KYC POLICY GUIDELINES

There are four key elements to the KYC guidelines as set out by RBI.

1. Customer Acceptance Policy
2. Customer Identification Procedures
3. Monitoring of Transaction, and
4. Risk Management

6.1 CUSTOMER ACCEPTANCE POLICY:

6.1.1 The GUIDELINES for Customer Acceptance Policy (CAP) for the Bank are given below:

a. No account is opened in anonymous/fictitious/benami name.

b. Accounts of persons with criminal background and/or having connections with terrorist organisations. Information relating to persons with criminal background and/or having contacts with terrorist organisations will be shared with the Branches from time to time. Branches will also have to be guided by the information available in the Planning and Development Section at Head Office for this purpose.

c. No account is opened where the Bank/Branch 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.

d. No transaction or account based relationship is undertaken without following the CDD procedure.

e. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified.

f. Optional/additional information is obtained with the explicit consent of the customer after the account is opened.

g. Bank/Branches shall apply Customer Due Diligence (CDD) procedure at the UCIC level. Thus, if an existing KYC complaint customer of a Bank/Branch desires to open another account with the same Bank/Branch, there shall be no need for a fresh CDD exercise.

h. CDD procedure is followed for all the joint account holders, while opening a joint account.

i. Circumstances in which, a customer is permitted to act on behalf of another personality/entity, is clearly spelt out.

j. The Bank shall put in place suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

k. For the purpose of risk categorisation of customer, the relevant information shall be obtained from the customer at the time of account opening. While doing so, it shall be ensured that information sought from the customer is relevant to the perceived risk and is not intrusive.

l. Customer Acceptance Policy shall not result in denial of Banking/financial facility to member of the general public, especially those, who are financially or socially disadvantage.

6.1.2 Branches should not open an account and should close an existing account, where the Branch is unable to apply appropriate customer due diligence measures, i.e. Branch is unable to verify the identity and / or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Bank. However, the decision to continue or close an existing account should be taken by the Officer only after he is satisfied with the process/documentation and in case of closure after giving 15 days notice to the customer explaining the reasons for such a decision, under intimation to the Principal Officer.

6.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP):

6.2.1 Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Sufficient information needs to be obtained to the satisfaction, which is necessary to establish the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Satisfaction means to be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

i. Customer Identification Procedure to be carried out at different stages:
   (a) While establishing a Banking relationship (or)
   (b) Carrying out a financial transaction (or)
   (c) When there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

ii. Identity to be verified for:

(a) The named account holder
(b) Beneficiary account
(c) Signatories to an account
(d) Intermediate parties

iii. For customers that are natural persons, sufficient identification data shall be obtained to verify:

(a) The identity of the customer
(b) His/her address/location
(c) His/her recent photograph and
(d) Document/s for verifying signature. In case no document is available for verification of the signature, Branch Head shall obtain the signature in his/her presence. Alternately, identity documents can be substituted by satisfactory personal introduction, except obtaining of photograph.

iv. For customers that are legal persons or entities:

(a) Legal status of the legal person/entity through proper and relevant documents shall be verified;
(b) It shall be verified that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person;
(c) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

v. The Bank shall identify the Beneficial Owner(s) and take all steps to verify his/her/their identity and capture the same in CBS.

vi. While opening the account of the customer or during periodic updation, Bank shall seek 'mandatory' information required for KYC purpose and for risk categorisation, which the customer is obliged to give. After the account is opened, the Bank may seek separately, other 'optional' details/additional information from the customer in his/her explicit consent.

vii. When there shall be any suspicion of money laundering or financing of the activities relating to terrorism or where there shall be any doubt about the adequacy or veracity of previously obtained customer identification data, the due diligence measures shall be reviewed including verifying again the identity of the client and obtaining information regarding purpose and intended nature of the business relationship.

viii. While opening the account of the customer or during periodic updation, only one documentary proof of address (either communication or permanent) may be obtained from the customer. In case the documentary proof of address furnished by the customer is not the local address or address where the customer is currently residing, Branches shall take a declaration of the local address on which all correspondence will be made by the Bank with the customer. This address shall be verified by the Bank through Positive Confirmation.

ix. In order to smoothen the Banking operations for the customers, bank shall have one unique Customer Information File (CIF) for all the accounts of a customer. A customer cannot have multiple CIF for various accounts opened at various locations of the Bank.

x. Customer identification data, including photograph(s), shall be periodically updated after the account is opened. Periodicity of such updation (obtaining full KYC) shall not be less than once in ten years in case of low risk category customers, not less than once in eight years in case of medium risk categories and not less than once in two years in case of high risk categories. Fresh photograph will be required to be obtained from minor customers on becoming major.

xi. The Bank need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect shall suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post etc. The Bank shall not insist on physical presence of such low risk customer at the time of periodic updation.

xii. In case of non-compliance of KYC requirements by the customers, despite repeated reminders, the Bank shall apply freeze by disallowing all debits and allowing only credits in such KYC compliant accounts in a phased manner after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing', the Bank shall disallow all debits and credits from/to the accounts. The Bank can also exercise option of closing such KYC non-compliant accounts.

6.3 CUSTOMER DUE DILIGENCE (CDD) PROCEDURE:

6.3.1 Customer Due Diligence:

Customer Due Diligence (CDD) can be defined as any measure undertaken by the Bank to collect and verify information provided by the customer and positively establish the identity of the customer. As listed in the IBA guidelines,

the Account Opening Officer must perform CDD on the customer when the Bank:

1. Establishes a new business relationship;
2. Carries out an occasional transaction;
3. Suspects money laundering or terrorist financing; or
4. Doubts the authenticity of the documents, data or information previously obtained for the purpose of identification or verification.

Similarly as outlined in the IBA guidelines, if the Account Opening Officer is unable to apply relevant due diligence measures, he or she

1. Must not establish a business relationship or carry out an occasional transaction with the customer;

2. Should not carry out a transaction with or for a customer through a bank account;

3. Should freeze or terminate all existing business relationships with the customer; and

4. Should consider reporting it to FIU-IND or to the regulators, in accordance with the guidelines.

6.3.2 Procedure for obtaining Identification Information:

(a) From an individual, who is eligible for enrolment of Aadhaar, the Aadhaar number; the Permanent Account Number (PAN) or Form No. 60, as defined in Income Tax Rules, 1962, as amended from time to time:

Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained:
Explanation: Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity.

Provided further, that from an individual, who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and who does not submit Aadhaar or proof of application of enrolment for Aadhaar, the following shall be obtained:

i) certified copy of an OVD containing details of identity and address and ii) one recent photograph

(b) From an individual, who is not eligible to be enrolled for an Aadhaar number, or who is not a resident, the following shall be obtained:

i) PAN or Form No. 60 as defined in Income Tax Rules, 1962, as amended from time to time.

ii) One recent photograph and

iii) A certified copy of an OVD containing details of identity and address:

Provided that in case the OVD submitted 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.

Provided further that, while opening accounts of legal entities, in case, PAN of the authorised signatory or the power of attorney holder is not submitted, the certified copy of OVD of the authorised signatory or the power of attorney holder shall be obtained, even if such OVD does not contain address.

Explanation 1: Aadhaar number shall not be sought from individuals who are not 'residents'.

Explanation 2: A declaration to the effect of individual not being eligible for enrolment of Aadhaar may be obtained by the Branches.

Explanation 3: Customers, at their option, shall submit one of the five OVDs.

(c) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have current address, an OVD (Passport, Driving Licence, Voter's ID issued by the Election Commission of India, Job Card issued by NREGA duly signed by an Officer of the State Government, Letter issued by the National Population Register containing details of name and address) shall be obtained from the customer for this purpose.

Provided that in case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

i) Utility Bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii) Property or Municipal tax receipt

iii) Pension or Family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address.

iv) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, Scheduled Commercial Banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

Provided further that the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

(d) Banks, at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.

Provided:

i) Yes/No authentication shall not be carried out while establishing an account based relationship.

ii) In case of existing accounts where Yes/No authentication is carried out, Branches shall ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/no authentication.

iii. Yes/No authentication in respect of beneficiary owners of a legal entity shall suffice in respect of existing accounts or while establishing an account based relationship.

iv. Where OTP based authentication is performed in 'non-face to face' mode for opening new accounts, the limitations as specified in Para 6.3.9 (Accounts opened using OTP based e-KYC, in non face to face mode) of this policy shall be applied.

v. Biometric based e-KYC authentication can be done by Bank official/business correspondents/business facilitators / Biometric enabled ATMs.

Explanation 1: While seeking explicit consent of the customer, the consent provisions as specified in Section 5 and 6 of the Aadhaar (Authentication) Regulations, 2016 shall be observed.

Explanation 2: Banks shall allow the authentication to be done at any of their Branches.

(e) In case the customer eligible to be enrolled for Aadhaar and obtain a PAN, does not submit the Aadhaar Number/Form 60 at the time of commencement of an account based relationship with a Branch, the customer shall submit the same within a period of six months from the date of the commencement of the account based relationship. In case the customer fails to submit the Aadhaar Number or PAN/Form 60 within the aforesaid six months period, the said account shall cease to be operational till the time the Aadhaar number and PAN/Form 60 is submitted by the customer.

Explanation: In case of asset accounts, such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed;

(f) Branches shall duly inform the customer about this provision while opening the account.

(g) The customer, eligible to be enrolled for Aadhaar and obtain the PAN, except one who is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, already having an account based relationship with Branches, shall submit the Aadhaar number and PAN/Form 60 by such date as may be notified by the Central Government. In case the customer fails to submit the Aadhaar Number and PAN/Form 60 by such date, the said account shall cease to be operational till the time the Aadhaar number and PAN/Form 60 is submitted by the customer.

(h) Branches shall ensure that introduction is not to be sought while opening accounts.

The Bank will perform three types of Due Diligence, as follows:

6.3.3 Basic Due Diligence:

All customers at the Bank must provide officially valid documents as a part of the account opening process in order to fulfill their KYC requirements. The documents required are based on the constitution, category and risk categorisation score of the customer. All low and medium risk customers must undergo Basic Due Diligence (BDD).

6.3.4 Simplified Due Diligence (SDD):

While the current policy has been designed to provide adequate flexibility in the collection of KYC information and documentary evidence, it has been observed that in certain cases customers, especially low income groups, are not able to provide the documentary evidence required by the Basic Due Diligence process. RBI guidelines recommend that banks do not exclude financially weaker sections of society from access to banking services because of the KYC, AML and CFT requirements.

Any CDD measures less stringent than the Basic Due Diligence measures are termed as Simplified Due Diligence (SDD).

6.3.5 Enhanced Due Diligence (EDD)

Any CDD measures more stringent than the Basic Due Diligence measures are termed as Enhanced Due Diligence (EDD). The policy requires the Account Opening Officer (AOO) to perform EDD on high risk customers identified as part of the Customer Risk Categorisation process.

Any system deployed for KYC information management at the Bank should be designed to transparently add on the EDD section based on the risk categorisation of the account.

6.3.6

Steps to perform EDD:

If the customer categorisation score is low or medium, no EDD is required on the customer. The steps for performing enhanced due diligence on high risk customers are as follows:

1. The AOO must request the customer for any additional information required;

2. Introducer's information, Source of funds, Additional photo ID, Additional Address proof, Purpose of account in the case of Current Accounts (whether individual or institutional), Products and services offered in the case of Current Accounts opened for the purpose of business, Address in Home Country in the case of non-resident accounts, Anticipated activity are indicative examples for Additional information to be obtained to complete EDD;

3. If the customer fails to provide the information requested as part of the EDD process, the BCM / BM must be notified with a recommendation for an exception or a one for account closure;

4. If the customer provides the required information, the AOO must review the information provided for accuracy, completeness and consistency with available information on the customer. If the information is found satisfactory, the AOO may open the account for the customer; and

5. As part of follow-up, the AOO or the BM, in certain cases may send a letter of thanks by registered post to the recorded address of the customer as well as the introducer. This would serve as a relationship building exercise and also allow the Bank to indirectly verify the address provided by customer as well as the introducer.
In case the letter is not delivered and returned to the Bank, the Bank must try and contact the customer or the introducer to determine the reason for the return and update the information accordingly. If no contact is possible and further information is not received, the account must be closed.

6. No customer once classified as high risk is exempt from the EDD process.

6.3.7 Documents in Languages other than English

If the customer provides a document in a language that the AOO cannot read and understand, he or she must use an internal translation resource to obtain a translation of the document in either English or Tamil. At a minimum, the translation must include the full customer name, a description of the type of document, the date of document and a reference to the content of the document. The translation must also include the name and designation of the translator within the bank.

6.3.8 CDD Procedure in case of Individuals:

Branches shall apply the following procedure while establishing an account based relationship with an individual:

(a) Obtain information as mentioned under para 6.3.2. [(a) to (h)] and

(b) Such other documents pertaining to the nature of business or financial status specified by the Bank in their KYC policy.

Provided that 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. Explanation: CDD procedure, including Aadhaar authentication and obtaining PAN/Form 60 as applicable, shall be carried out for all the joint account holders.

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

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

ii. The aggregate balance of all the deposit accounts of the customer shall not exceed Rs. 1 lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

iii. The aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed Rupees 2 lakhs.

iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Biometric based e-KYC authentication is to be completed.

vi. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts, no further debits shall be allowed.

vii. Branches shall ensure that only one account is opened using OTP based KYC in non face to face mode and a declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non face to face mode. Further, while uploading KYC information to CKYCR, Banks shall clearly indicate that such accounts are opened using OTP based e-KYC and other Banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non face to face mode.

viii. Banks shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

6.3.10 Small Account:

(i) Small Account means a Savings account in a Banking company where:-

(a) the aggregate of all credits in a financial year does not exceed Rs. 1 lakh.

(b) the aggregate of all withdrawals and transfers in a month does not exceed Rs. 10000/- and

(c) the balance at any point of time does not exceed Rs. 50000/-

(ii) In case an individual customer, who does not have Aadhaar/enrolment number and PAN and desires to open a Bank account, Banks shall open a 'Small Account', subject to the following:

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

(b) The designated officer of the Bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) Such accounts are opened at Core Banking Solution linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

(d) Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place

(e) The account shall remain operational initially for a period of 12 months which can be extended for a further period of 12 months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first 12 months of the opening of the said account.

(f) The entire relaxation provisions shall be reviewed after 24 months.

(g) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of an OVD and Aadhar Number or where an Aadhaar number has not been assigned to the customer through the production of proof of application towards enrolment for Aadhaar which is not more than six months old, along with an OVD.

(h) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of an OVD and Aadhaar Number or the enrolment number which is not more than six months old, where the person is eligible to enroll for Aadhaar number has not been assigned an Aadhaar number.

Provided that if the client is not eligible to be enrolled for the Aadhaar number, the identity of client shall be established through the production of an OVD.

6.3.11 CDD Measures for SOLE PROPRIETARY FIRMS:

For opening an account in the name of a sole proprietary firm, identification information, as mentioned under Section 15 in respect of the individual (proprietor) shall be obtained.

In addition to the above, any two of the following documents as a proof of business/activity in the name of the proprietary firm shall also be obtained:

(a) Registration Certificate

(b) Certificate/Licence issued by the Municipal Authorities under Shop and Establishment Act

(c) Sales and Income Tax Returns

(d) CST/ VAT/GST Certificate (provisional/final)

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax Authorities.

(f) Importer Exporter Code (IEC) issued to the proprietary concern by the office of DGFT/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 and landline telephone bills.

6.3.12 CDD Measures for Legal Entities:

i. For opening an account of a COMPANY, certified copies of each of the following documents shall be obtained:

(a) Certificate of incorporation

(b) Memorandum and Articles of Association

(c) A Resolution from the Board of Directors and Power of Attorney granted to its Managers, Officers or employees to transact on its behalf.

(d) Identification information as mentioned under Section 15 in respect of Managers, Officers or employees holding an attorney to transact on its behalf.

(e) Copy of the PAN allotment letter.

(f) Copy of the Telephone Bill

ii. For opening an account of a PARTNERSHIP FIRM, certified copies of each of the following documents shall be obtained:

(a) Registration certificate

(b) Partnership Deed

(c) Identification information as mentioned under Section 15 in respect of the person holding an attorney to transact on its behalf.

(d) Photographs of partners

(e) Telephone Bill/Utility Bill in the name of firm/Partners.

iii. For opening an account of a TRUST, certified copies of each of the following documents shall be obtained:

(a) Registration Certificate

(b) Trust Deed

(c) Identification information as mentioned under Section 15 in respect of the person holding an attorney to transact on its behalf.

(d) Resolution of the Managing body to open an account

(e) Copy of PAN Card

(f) Copy of Telephone Bill

iv. For opening an account of an UNINCORPORATED ASSOCIATION or a BODY OF INDIVIDUALS, certified copies of each of the following documents shall be obtained:

(a) Resolution of the Managing Body of such Association or Body of Individuals.

(b) Power of attorney granted to transact on its behalf.

(c) Identification information as mentioned under Section 15 in respect of the person holding an attorney to transact on its behalf and

(d) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association' Explanation: Term 'body of individuals includes societies.

v. For opening accounts of JURIDICAL PERSONS not specifically covered in the earlier part, such as Government or its Departments, Societies, Universities and local bodies like Village Panchayats, certified copies of the following documents shall be obtained:

(a) Document showing name of the person authorised to act on behalf of the entity:

(b) Aadhaar/PAN/Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and

(c) Such documents as maybe required by the Bank to establish the legal existence of such an entity/juridical person.

6.3.13 IDENTIFICATION OF BENEFICIAL OWNER:

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 Rule 9(3) of the Rules (as specified in 4.2 Beneficial Owner) to verify his/her identity shall be undertaken keeping in view the following:

(a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) In cases of Trust/nominee of 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.

6.3.14 HINDU UNDIVIDED FAMILY (HUV) ACCOUNTS:

HUF comes into being because of a particular concept under Hindu Law, whereby all the members of the family reside together jointly, carry on a business activity jointly and hold the property jointly and therefore, it is termed as Hindu Undivided Family

(a) Declaration from the Karta

(b) Proof of identification of Karta

(c) Prescribed Joint Hindu Family letter signed by all the adult CoParceners.

(d) Permanent Account Number in the name of Karta.

(e) Identification information as mentioned under Section 15 in respect of Karta and other Co-Parceners.

6.3.15 MINOR ACCOUNTS:

The branches may open accounts in the name of Minors, subject to the following:

(a) A Savings/Fixed/Recurring Deposit account can be opened by a minor of any age through his/her natural or legally appointed guardian.

(b) Minors above the age of 10 may be allowed to open and operate savings bank account independently, if they so desire.

(c) On attaining majority, the erstwhile minor should confirm the balance in his/her account and if the account is operated by the natural guardian/legal guardian, fresh operating instructions and specimen signature of erstwhile minor should be obtained and kept on record for all operational purposes.

(d) Branches may consider extending additional Banking facilities like Internet Banking, ATM Debit Card, Cheque Book etc. subject to the safeguards that minor accounts are not allowed to be overdrawn and that these always remain in credit.

(e) Often a family member or guardian would open an account for a minor. In cases where the adult opening the account does not already have an account with the Bank, the identification proof for that adult or any other person who will operate the account should be obtained. In case of self operated minor accounts, in addition to the photograph and proof of age, the documents required to establish the identity and address applicable in the case of individuals be obtained.

6.3.16 SOCIETY/ASSOCIATION/CLUBS:

In the case of applications received on behalf of societies/ associations/clubs, the Officer should take reasonable steps to satisfy himself as to the legitimate purpose of the organisation by going through the constitution. The identity of the authorised signatories should be verified initially in line with the requirements for personal customers. When signatories change, care should be taken to ensure that the identity of any new signatories has been verified.

(a) While the set of documents as stated above should normally suffice to establish both the identity and the correct address of the applicant, wherever this is not so, applicants have to be asked to give additional documents with the satisfaction of the Officer.

(b) Based on materiality and risk, verification of beneficial owners, directors, may not be taken for significant and well established entities, companies listed on recognized investment / stock exchanges, government departments or their agencies, government linked companies, statutory corporations.

6.3.17 EDD FOR ACCOUNTS OF POLITICALLY EXPOSED PERSONS (PEPs):

Branches shall have the option of establishing a relationship with the Politically Exposed Persons, provided that

(a) Sufficient information, including information about the sources of funds, accounts of family members and close relatives is gathered on the PEPs.

(b) The identity of the person shall have been verified before accepting the PEP as a customer.

(c) The decision to open an account for a PEP is taken at a senior level in accordance with the Bank's Customer Acceptance Policy.

(d) All such accounts are subjected to enhanced monitoring on an on-going basis

(e) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, Senior Management's approval is obtained to continue the business relationship

(f) The CDD measures as applicable to PEPs, including enhanced monitoring on an on-going basis are applicable.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

6.3.18 SDD FOR SELF HELP GROUPS (SHGs):

(a) CDD of all the members of SHG as per the CDD procedure mentioned in Para 6.3.2. [(a) to (h)] (Procedure for Obtaining Identification Information) shall not be required while opening the Savings Bank account of the SHG.

(b) CDD as per the CDD procedure mentioned in Para 6.3.2. [(a) to (h)] of all the Office bearers shall suffice.

(c) No separate CDD as per the CDD procedure mentioned in Para 6.3.2. [(a) to (h)] of the members or office bearers shall be necessary at the time of credit linking of SHGs.

6.4 MONITORING OF TRANSACTIONS:

(a) It is important to recognize that the KYC is an ongoing process.

(b) The Officer should closely monitor the following accounts.

i) High Risk Accounts

ii) Accounts involving large amounts of cash transactions inconsistent with the normal/expected activity in the account.

iii) Transactions on newly opened accounts

iv) Regular transfers between group/related accounts

v) Large value transactions in accounts, which are inconsistent with the profile/nature of business of the customer.

vi) The officer should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

6.5 ON-GOING DUE DILIGENCE:

(a) Officers of Branches shall undertake ongoing 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.

(b) Without prejudice to the generality of factors that call for close monitoring, the following types of transactions shall necessarily be monitored.

i) 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.

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

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

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

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

(d) High Risk accounts have to be subjected to more intensified monitoring:

i) A system of periodic review of risk categorisation 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.

ii) The transactions in accounts of marketing firms, especially accounts of Multi-Level Marketing (MLM) Companies shall be closely monitored.

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.

6.6 PERIODIC UPDATION:

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers, as per the following procedure:

(a) Officers shall carry out:

i) PAN verification from the verification facility available with the issuing authority and

ii) Authentication of Aadhaar Number already available with the Bank with the explicit consent of the customer in applicable cases.

iii) In case identification information available with Aadhaar does not contain current address, an OVD containing current address may be obtained.

iv) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorised as 'low risk'. In case of low risk customers, when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

v) In case of legal entities, the Officers shall review the documents sought at the time of opening of account and obtain fresh certified copies.

(b) The Officers at the Branches may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bonafides. Normally, OVD/Consent forwarded by the customer through mail/post etc. shall be acceptable.

(c) The Officers at the Branches shall ensure to provide acknowledgement with date of having performed KYC updation.

(d) The time limits prescribed above would apply from the date of opening of the account/last verification of KYC.

6.7 CUSTOMER PROFILE:

6.7.1 For the purpose of exercising due diligence on individual transactions in accounts, "customer Profile" of individual account holders be compiled in addition to the account opening forms.

6.7.2 Customer profiles have to be prepared for all accounts (deposit/loan).

a. When the Officer feels it is necessary to obtain additional information from existing customer based on the conduct or behaviour of the account.

b. While opening accounts by transfer from other branches, the customer profile may be updated.

6.7.3 Care to be exercised that:

a. Implementation of the KYC guidelines should not result in denial of banking services (including opening of account) to the public, especially to those, who are financially or socially disadvantaged.

b. Introduction of large number of accounts by a single introducer (either account holder or staff) to be accepted with caution.

c. In the case of existing account holders, KYC procedures have to be completed for high and medium risk accounts while opening and /or renewal of term/recurring deposits, if not already done except in cases where the deposits are placed with the banks under auto renewal procedure or issued to the debit of an existing account.

d. while opening bank accounts and during periodic updating of the customer at the time of periodic updating;

- do not insist on physical presence of the customer at the time of periodic updating;
- do not seek fresh proof of identity and address at the time of periodic updating in case of no change in status for 'low risk' customers; allow self-certification; accept a certified copy of the document by mail/post, etc; and
- do not seek fresh documents if an existing KYC compliant customer of a bank desires to open another account in the bank.

e. The information collected from the customer will be treated as confidential and not divulge any details thereof for cross selling or any other purposes.

f. The KYC guidelines are applicable to all new technology products of the Bank, like issue of ATM Card.

6.8 RISK MANAGEMENT:

6.8.1 The level of money laundering risks that the Bank is exposed to by a customer relationship depends on:

a. Type of the customer and nature of business
b. Type of product / service availed by the customer
c. Country where the customer is domiciled.

Based on the above criteria, the customers are being classified into three money laundering risk levels.

The Bank has fixed certain minimum standards of account documentation for all new customer relationships, to enable the Bank to understand the nature of the customer's business, carry evidence of key data regarding the customer and its principal owners/signatories and understand the type and level of activity that is to be considered as normal in the customers' account.

6.8.2 Three types of Money Laundering Risk Levels:

Customers may be classified in various categories as under:

6.8.2.1 High Risk:

a. who are engaged in certain professions where money laundering possibilities are high. Eg. Antique Dealers (individuals and entities), Money Services Bureau (entities – not employees of these entities) and dealers in arms

b. who live in 'High Risk Countries' (nationality is irrelevant).

c. Politically Exposed Persons (PEP) of foreign origin – Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government / judiciary / military officers, senior executive of state owned corporations, important political party officials, etc. The Bank should obtain additional information disclosing the source of funds that would be deposited in the account.

Opening of the above accounts would need specific approval of the Principal Officer.

6.8.2.2 Medium Risk:

Customers are classified as Medium if they qualify under the following parameters:

a. Any of the account holders lives in a Medium risk country.

b. Total aggregate credits to the account in excess of Rs.10.00 lakhs, other than customers where there is sufficient knowledge in the public domain, which will enable the Bank to classify such customers/categories of customers as Low Risk.

6.8.2.3 Low Risk:

All customers who are not High/Medium Risk are Low Risk customers. All borrowal customers (other than high risk category) where due diligence is done at the time of granting the facilities will fall under the low risk category. Illustrative example of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover. For low risk customers, the basic requirements of identity and location of the customer are only to be verified.

6.8.2.4 Extra Precaution to be taken in the opening of the following types of accounts:

The following types of accounts would require higher account opening documentation and due diligence to be carried out at the time of opening new accounts.

a. Non-resident customers

b. High Networth individuals
c. Trusts, Charities, NGOs and organisations receiving donations,
d. Companies having close family shareholding or beneficial ownership,
e. Firms with 'sleeping partners'.
f. Politically exposed persons (PEP) of foreign origin.
g. Those with dubious reputation as per public information available
h. Fiduciary accounts – opened by professional intermediaries like stockbrokers, Chartered Accountants, etc.

6.9. TRANSACTIONS OF SUSPICIOUS NATURE:

6.9.1 Satisfactory KYC procedures provide the foundation for recognizing unusual and suspicious transaction. Where there is a business relationship, a suspicious transaction will often be one that is inconsistent with a customer's known legitimate activities or with the normal business for that type of account

6.9.2 A transaction or a series of transactions would be considered 'suspicious' if the transaction(s) appears to be inconsistent with the customer's legitimate business or personal activities or known transaction profile or if it does not make economic sense.

6.9.3. The courteous approach in the process is very essential to take care that the customers are not driven away from the Bank. However, care should be taken to ensure that customers are not tipped off that their account(s) are under transaction monitoring.

6.9.4 The Bank shall furnish to the Director, Financial Intelligence UnitIndia (FIU-IND) information referred to in Rule 3 of the PML (Maintenance of Records) Rules 2005 in terms of Rule 7 thereof {as specified in Para 6.11 [(a) to (f)]}

6.10. TERRORIST FINANCE:

List of terrorist organisations/banned organisations circulated by RBI from time to time would require to be consulted to check existence of account of such organisation and initiate appropriate action before opening of any new accounts in future and the list to be made available at all counters. The Officers should not open any account in the names of terrorist / banned organisations.

6.11 MAINTENANCE OF RECORDS OF TRANSACTION (NATURE AND VALUE)

As per Rule 3 of PML Act, the Officers at the Bank shall maintain proper record of all transaction, including the following:

(a) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.

(b) All series of cash transactions integrally connected to each other which have been below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

(c) All cash transactions where forged or counterfeit currency notes or Bank notes have been used as genuine and where any forgery of a valuable security has taken place.

(d) All suspicious transactions whether or not made in cash and by way of:

i. Deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:

- Cheques including third party cheques, pay orders, demand drafts, or any other instruments of payment of money including electronic receipts or credits and electronic payments or debits, or
- Travelers cheques or
- Transfer from one account within the same Branch / Bank, or
- Any other mode in whatsoever name it is referred to.

ii. Credits or debits into or from any non-monetary accounts such as 'demat' account, security account in any currency maintained by the Branch.

iii. Money transfer or remittances in favour of own clients or nonclients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by way of the following:

- Payment order
- Demand draft
- Telegraphic or wire transfers or electronic remittances or transfer
- Internal transfers
- Automated Clearing House remittances
- Any other mode of money transfer by whatsoever name it is called.

iv. Loans and advances including credit or loan substitutes, investments and contingent liability by way of the following:

- Subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter-Bank participation or any other investments in securities or the like in whatever form and name it is referred to
- Purchase and negotiation of bills, cheques and other instruments
- Foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called

- Letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and or credit support.

v. Collection services in any currency by way of collection of bills, cheques instruments or any other mode of collection in whatsoever name it is referred to.

(e) 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.

(f) All purchase and sale by any person of immovable property valued at Rs. 50 lakhs or more that is registered by the reporting entity, as the case may be.

6.12 RECORDS CONTAINING INFORMATION:

(a) The records referred to in Para 6.11 [(a) to (f)] shall contain the following information.
i. the nature of the transactions
ii. the amount of the transaction and the currency in which it was denominated.
iii. the data on which the transaction was conducted and iv. the parties of the transaction

(b) The Branch shall maintain information in respect of transactions with its customers referred to in Para 6.11 [(a) to (f)] in hard and soft copies.

6.13 RECORD MANAGEMENT:

The following steps shall be taken by the Officers at the branches regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules:

(a) To 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;

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

(c) To make available the identification records and transaction data to the competent authorities upon request;

(d) To introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules 2005.

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

i) the nature of the transactions ii) the amount of the transaction and the currency in which it was denominated.
iii) the date on which the transaction was conducted; and iv) the parties to the transaction.

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

(g) To maintain records of the identity and address of their customers and records in respect of transactions referred to in Rule 3 of PML Rules 2005 in hard and soft format.

6.14 PROCEDURE AND MANNER OF FURNISHING INFORMATION:

i. The Bank shall communicate the name, designation and address of the Principal Officer to the Director.

ii. The Branch shall furnish the information referred to in Para 6.11 [(a) to (f)] every month to the Principal Officer by the 5th day of succeeding month other than transactions referred to in clauses (c), (d) of Para 6.11 above.

Provided that information in respect of transactions referred to in clauses (c) and (d) shall be promptly furnished in writing to the Principal Officer immediately on the date of occurrence of such transactions.

iii. The Principal Officer shall furnish the information referred to in Para 6.11 to the Director on the basis of information available with the Bank. A copy of such information shall be retained by the Principal Officer for the purpose of official record.

iv. The Principal Officer shall furnish the information in respect of transactions referred to in Para 6.10 every month to the Director by the 7th day of succeeding month other than transactions referred to in clauses (c), (d) of Para 6.11.

Provided that information in respect of transactions referred to in clauses (c) and (d) shall be promptly furnished in writing by the Principal Officer by way of fax or electronic mail to the Director not later than three working days from the date of occurrence of such transactions.

6.15 REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-IND):

6.14.1 As per the requirement of PMLA, 2002 and the rules thereunder, the following information shall be furnished to FIU-IND.

a) All cash transactions of the value of more than Rs. 10 lakhs or its equivalent in foreign currency.

b) All series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs. 10 lakhs or its equivalent in foreign currency.

c) All transactions involving receipts by non-profit organisations of value more than Rs. 10 lakh or its equivalent in foreign currency.

d) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions

e) All suspicious transactions whether or not made in cash; and

f) As per Rule 3(e) of PMLA, all cross border wire transfers of the value of more than Rs. 5 lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India.

6.14.2 A profile for each customer based on the risk categorisation shall be prepared. As a part of transaction monitoring mechanism, an appropriate software application is to be put in place to trigger alerts when the transactions are inconsistent with risk categorisation and updated profile of customers.

6.14.3 As per Rule 8(4) of the PMLA, while furnishing of 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 this rule shall constitute a separate violation.

6.16 VARIOUS REPORTING FORMATS:

6.16.1 CASH TRANSACTION REPORT:

(a) Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting is done centrally by the Bank and is submitted on a monthly basis to FIU-IND within the prescribed time schedule.

(c) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported on monthly basis by the Principal Officer to FIU-IND in a specified format by 15th of the succeeding month (Counterfeit Currency Report – CCR). These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and shall be reported to FIU-IND in plain text form.

(d) While filing CTR, details of individual transactions below Rs.50000/- need not be furnished.

(e) CTR contains only the transactions carried out on behalf of clients/customers excluding transactions between the internal accounts of the Bank.

(f) A summary of cash transaction report for the Bank as a whole is complied by the principal Officer every month as per the format specified. The summary is submitted online by the Principal Officer to FIU-India.

(g) The monthly CTR submitted centrally to FIU-India is accessible by the concerned branch for production to auditors/inspectors, when asked for.

6.16.2 SUSPICIOUS TRANSACTION REPORTS (STR):

(a) While determining suspicious transactions, Banks shall be guided by definition of suspicious transaction contained in para 4.4 above as amended from time to time.

(b) In some cases, transactions may be abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted

transactions should be reported in STRs, even if not completed by customers, irrespective of the amount of the transaction.

(c) STRs shall be made if there is reasonable ground to believe that the transaction generally involves proceeds of crime irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA 2002.

(d) The STR shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his/her reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

(e) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions.

(f) No restrictions shall be put on operations in the accounts where an STR has been made. The fact of furnishing of STR shall be kept strictly confidential, as required under PML Rules. Customer shall not be tipped off at any level.

6.16.3 NON-PROFIT ORGANISATION (STR):

The report of all transactions involving receipts by non-profit organisations of value more than Rs. 10 lakh or its equivalent in foreign currency shall be submitted every month in the prescribed format.

6.17 TRAINING:

The Bank, in consultation with ACSTI, shall have an ongoing training programme so that members of the staff are adequately trained on KYC procedures. Training requirements should adequately focus on frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

-:o:-

The Erode Dist Central Co-op. Bank Ltd. HEAD OFFICE ERODE

MANAGING DIRECTOR 26/7/23