

**Policy on Know Your Customer (KYC) Standards, Anti-Money Laundering (AML) and Combating Financial Terrorism (CFT) Measures**  
**INDEX**

	Pg.Nos.
1. Preamble	1
2. Objective, Scope & Application	1
3. Definition of Money Laundering	2
4. Obligations under Prevention of Money Laundering Act, 2002	2-4
5. Risk Perception	4
6. Definition of a Customer	5
7. Key Elements of the Policy	5
7.1 Customer Acceptance Policy (CAP)	6-9
7.2 Indicative Guidelines	9-16
7.3 Customer Identification Procedures (CIP)	16-17
7.4 Small Deposit Accounts	17-22
7.5 Monitoring & Reporting of Transactions	22-23
7.6 Closure of Accounts	23
7.7 Risk Management	23
8. Employee Training	23
9. Recruitment/Hiring of Employees	23
10. Customer Education	23
11. Introduction of New Technologies	23
12. KYC for the existing accounts	23
13. Record Keeping	24
14. Retention of Records	24
15. Correspondent Banking	25
16. Miscellaneous	25
17. Principal Officer	25
18. Review of the Policy	25
19. Duties and Responsibilities and Accountability	26
Annexure I Transactions of suspicious nature	27-32
Annexure II Duties and Responsibilities and Accountability	33-34

## **Model Policy on Know Your Customer (KYC) Standards and Anti Money Laundering (AML) /Combating Financing of Terrorism (CFT) Measures**

### **1. Preamble**

Reserve Bank of India and NABARD have been issuing guidelines in regard to Know Your Customer (KYC) standards to be followed by banks and measures to be taken in regard to Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT). The guidelines incorporate the:

- Obligations cast on banks under the Prevention of Money Laundering Act (PMLA), 2002
- Recommendations made by the Financial Action Task Force (FATF) on AML standards and CFT
- Paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision

Cooperative and Regional Rural Banks are required to put in place a comprehensive policy framework, duly approved by the Board of Directors, in this regard. This draft policy document has been prepared in line with the RBI/NABARD guidelines and incorporates the Bank's approach to KYC, AML and CFT issues.

### **2. Objectives, Scope and Application of the Policy:**

- The primary objective of the Policy is to prevent the Cooperative/Regional Rural Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. Purposes proposed to be served by the Policy are:

(i) To prevent criminal elements from using the Cooperative/Regional Rural Bank for money laundering activities

(ii) To enable the Cooperative/Regional Rural Bank to know/ understand the customers and their financial dealings better which, in turn, would help the bank to manage risks prudently

(iii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

(iv) To comply with applicable laws and regulatory guidelines.

(v) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

This Policy is applicable to all branches/offices of the Cooperative/Regional Rural Bank and is to be read in conjunction with related operational guidelines issued from time to time.

### **3. Definition of Money Laundering**

Section 3 of PMLA has defined the "offence of money laundering" as under:

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

Money launderers use the banking system for cleansing 'dirty money' obtained from criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds.

For the purpose of this document, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

### **4. Obligations under Prevention of Money Laundering (PML) Act 2002**

Section 12 of PMLA places certain obligations on every banking company, financial institution and intermediary, which include

- (i) Maintaining a record of prescribed transactions
- (ii) Furnishing information of prescribed transactions to the specified authority
- (iii) Verifying and maintaining records of the identity of its clients
- (iv) Preserving records in respect of (i), (ii) and (iii) above for a period of ten years from the date of cessation of transactions with the clients.

These requirements have come into effect from the 1<sup>st</sup> July, 2005 i.e. the date on which PMLA was notified by the Government of India and rules framed thereunder.

### **Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Amendment Rules, 2009 - Obligation of Banks/Financial Institutions**

The Government of India vide its Notification No.13/2009/F.No.6/8/ 2009-ES dated November 12, 2009, has amended the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005.

2. Some of the salient features of the amendment, relevant to State and Central Co-operative banks/RRBs are as under:

Clause (ca) inserted in sub-rule (1) of Rule 2 defines "non-profit organization"

Clause (BA) inserted in sub-rule (1) of Rule 3 requires banks/ financial institutions to maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency.

The amended Rule 6 provides that the records referred to in rule 3 should be maintained for a period of ten years from the date of transactions between the client and the banking company/financial institution.

A proviso has been inserted in sub-rule (3) of Rule 8, which requires that banks and its employees should keep the fact of furnishing suspicious transaction information strictly confidential.

Rule 9, now requires banks to verify identity of the non-account based customer while carrying out transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

The amended sub-rule (1) of Rule 9, in terms of clause (b) (ii) requires verification of identity of the customer for **all** international money transfer operations.

Proviso to Rule 9 (1) regarding the verification of identity of the client within a reasonable time after opening the account/ execution of the transaction has been deleted.

"for clause (g), the following clause shall be substituted, namely:-

(g) " suspicious transactions" means a transaction referred to in clause (h) 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 have no economic rationale or bonafide purpose; or
- (c) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.”

3. Accordingly, in view of amendments to the above Rules, State and Central Co-operative Banks/RRBs are required to :

(i) Maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency and to forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15th of the succeeding month.

(ii) In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50, 000/- the bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

## **5. Risk Perception**

Non compliance with KYC standards, use of the portals of the Cooperative/Regional Rural Bank for Money Laundering/financing terrorism activities expose the Bank to various risks, such as, Operational Risk, Reputation Risk, Compliance Risk, Legal Risk, etc.

## **6. Definition of a Customer**

A customer, for the purpose of the Policy is defined as:

- (i) a person or an entity that maintains an account and/or has a business relationship with the Bank
- (ii) one on whose behalf the account is maintained (i.e. the beneficial owner)
- (iii) beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- (iv) any person or entity connected with a financial transaction which can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

## **7. Key Elements of the KYC Policy**

### **• KYC Policy includes the following nine key elements:**

1. *Customer Acceptance Policy (CAP)*
2. *Customer Identification Procedures (CIP)*
3. *Monitoring of Transactions*
4. *Risk management*
5. *Training Programme*
6. *Internal Control Systems*
7. *Record Keeping*
8. *Evaluations of KYC guidelines by internal audit and inspection system*
9. *Duties / Responsibilities and Accountability*

While the Policy directions are given in this document, the detailed operating guidelines are being issued separately which should be referred to for effective implementation of the Policy.

### **7.1 Customer Acceptance Policy**

Bank's Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Bank broadly are:

- (i) No account is to be opened in anonymous or fictitious/benami name(s)/entity(ies)
- (ii) Accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed later). Necessary checks before opening a new account are to be ensured so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available from Circulars, etc.
- (iii) Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorisation
- (iv) Documentation requirements and other information to be collected, as per PMLA and RBI/NABARD guidelines/instructions, to be complied with
- (v) Not to open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be

verified and/or documents/information required could not be obtained/confirmed due to non-cooperation of the customer

(vi) Identity of a new customer to be checked so as to ensure that it does not match with any person with known criminal background or banned entities such as individual terrorists or terrorist organizations etc.

(vii) Implementation of CAP should not become too restrictive and result in denial of banking services to general public, especially those who are financially or socially disadvantaged.

(viii) The decision to open an account for Politically Exposed Person (PEP) should be taken at a senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

(ix) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

## **7.2. Indicative Guidelines**

### **7.2.01 Trust/Nominee or Fiduciary Accounts**

Branch/offices should determine whether the customer is acting on behalf of another person as trustee/nominee or any other interme-diary. If so, branch/offices may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

While opening an account for a trust, branches/offices should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Beneficiaries should be identified when they are defined. In the case of a 'foundation', branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

### **7.2.02 Accounts of companies and firms**

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with banks. Branch/ office may examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and

who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

### **7.2.03 Client accounts opened by professional intermediaries**

When the Branch/office has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branch/office also maintain 'pooled' accounts managed by lawyers/ chartered accountants for funds held 'on deposit' for a range of clients.

Where funds held by the intermediaries are not co-mingled at the Branch/office and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the Branch/office, the bank should still look through to the beneficial owners. Where the Branch/ office rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

It should be understood that the ultimate responsibility for knowing the customer lies with the Branch/office.

### **7.2.04 Adherence to Foreign Contribution Regulation Act (FCRA), 1976**

Branches/Offices should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976 cautioning them to open accounts or collect cheques only in favour of association, which are registered under the Act ibid by Government of India. A certificate to the effect that the association is registered with the Government of India should be obtained from the concerned associations at the time of opening of the account or collection of cheques.

Branches/offices are advised to exercise due care to ensure compliance and desist from opening accounts in the name of banned organizations and those without requisite registration.

### **7.2.05 Accounts of Politically Exposed Persons(PEPs) \_\_\_\_\_ resident outside India**

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branch/office should gather sufficient information on any

person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

Branch/office should verify the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior level and should be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs

### **7.2.06. Correspondent Banking**

Relationships with correspondent banks should be established only with the approval of the Board.

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, Inter- national wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank.

Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance.

Similarly, branch/office should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action.

The responsibilities of the bank with which correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

Branches/Offices should ensure that their respondent banks have anti-money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts. Accept customers only after verifying their identity, as laid down in Customer Identification Procedures (discussed below).

### **7.2.07 Profile based on categorisation**

Branches/offices should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients. business and their location etc.

For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk.

Illustrative examples 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, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

Customers that are likely to pose a higher than average risk to the **bank** may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Enhanced due diligence measures are to be applied based on the risk assessment, thereby requiring intensive due diligence for higher risk customers, especially those for whom the sources of funds are not clear.

### **7.3 Customer Identification Procedures (CIP)**

Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Procedures (**CIP**) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship. This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions.

Identification data, as under, would be required to be obtained in respect of different classes of customers:

#### **7.3.01. For customers that are natural persons:**

- a) Address/location details
- b) Recent photograph

#### **7.3.02. For customers that are legal persons:**

- a) Legal status of the legal person/entity through proper and relevant

documents.

b) Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person/entity is established and verified.

c) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc. will be collected for completing the profile of the customer.

If the branch/office decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

### **7.3.03. For New Accounts**

"Know Your Customer" (KYC) procedure should be the key principle for identification of an individual/corporate opening an account. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer.

### **7.3.04. Customer Identification:**

***The objectives of the KYC framework should be two fold***

- 1. to ensure appropriate customer identification and*
- 2. to monitor transactions of a suspicious nature.*

Branches/offices should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves. Easy means of establishing identity would be documents such as passport, driving licence, etc. Where such documents are not available, verification by existing account holders or introduction by a person known to the bank may suffice.

### **7.3.05. Existing Accounts :**

With a view to ensuring that existing small account holders are not inconvenienced and the KYC procedures is completed in time, it has been decided that application of KYC procedures may be limited to the existing accounts, where the credit or debit summation for the financial year ended March 31, 2003 is more than Rs. 10.00 lakh or where the branch or office suspects any unusual transaction. However, branches/offices should fully

implement the KYC norms in all existing accounts of trusts, companies/firms, religious/charitable organizations and other institutions or where the accounts are opened through a mandate or power of attorney.

### **7.3.06. Introduction**

The customer identification will be through an introductory reference from an existing account holder/person known to the **Bank** and or on the basis of documents provided by the customer.

#### **Introduction in Rural and Semi-Urban branches**

The individuals in **rural and semi urban branches** can open deposit accounts by providing introduction from a third person having satisfactory conduct of the account for six months (barring new branches) or by well known local authorities or through staff members, against whom disciplinary proceedings are not pending, knowing the potential customer.

#### **Introduction in Urban and Metro centre branches**

In urban and metro centre branches, accounts to be opened on the basis of any one of the following:

An introduction from a third person having satisfactory conduct of the account for at least 12 months or by well known local authorities or through staff members knowing the potential customer.

Passport alone, may be accepted , when the address on the passport is the same as the address in the account opening form. Any other document from each of the undernoted two lists for a photo ID and proof of residence.

#### **List 1**

1. Passport where the address differs
2. Election ID Card\*
3. Pan Card\*
4. Govt./Defence ID Card
5. ID Cards of reputed employers
6. Driving Licence

#### **List 2**

1. Credit Card Statement\*\*
2. Salary Slip\*\*
3. Income/Wealth Tax Assessment Order
4. Electricity Bill\*\*
5. Telephone Bill\*\*

**\* With a self signed cheque drawn on existing **bank**.      \*\*  
Latest/recent**

Documents under List 1 will establish identity of the account holder and documents of List 2 will give present address of the account opener.

While the above set of documents should normally suffice to establish both the identity and the correct address of the applicant, wherever this is not so (e.g. PAN Card and Salary Slip together may not provide proof of address) applicants to be asked to give additional documents e.g. a letter from the employer giving the correct address, credit card statement etc. In case of joint account, applicants who are not closely related to each other would require to establish their identity and address independently.

In respect of NRI accounts, introduction and authentication/ verification of signatures to be made by a bank/Indian embassy/ High Commissioner/ Consulate/ Notary Public/ Persons known to the bank.

For establishing identity or proof of residence Ration Card should not be used as document. However, in the event of non-availability of any other document, Ration Card may also be accepted as proof of residence from minors/illiterate persons who are unable to produce other documents.

### **7.3.07. Other than individual accounts**

Accounts on behalf of the following customers to be opened by our branch/office after obtaining documents stated against their names and any other documents/introduction that branch/office feel necessary to comply with KYC guidelines.

**Company** – Certificate of Incorporation, Memorandum and Articles of Association, Certificate of commencement of business where required and a copy of the resolution of the Board of Directors for opening of account.

**Society/Associates/Clubs** – Resolution for opening of the account and a copy of bye-laws and certificate of registration in case of registered clubs, societies and associations.

**HUF** – Declaration from the Karta.

**Trust** – A copy of the resolution, trust deed and a copy of registration certificate.

**Firms** – In the case of Partnership firm, partnership letter and introduction from a person known to the bank.

### **7.3.08. Letter of thanks**

In all instances of opening of new accounts letter of thanks to be sent by registered post at the recorded addresses to all customers and introducers with dual purpose, thanking them for opening the account with the Bank and for verification of genuineness of address furnished by the account holder. Undelivered envelopes in this regard would be required to be followed up closely at branch levels.

The operating staff/ officers associated with opening of accounts would be required to exercise due diligence and care at the time of opening of accounts. Care should, however, be taken that implementation of KYC guidelines do not result in denial of opening of new accounts.

### **7.3.02. Customer Profile**

*Care to be exercised that implementation of the KYC guidelines should not result in denial of opening of new accounts at the branches. Nevertheless, customer profiles to be compiled without exception.*

For the purpose of exercising due diligence on individual transactions in accounts, 'Customer Profile' of individual account holders in the account should be incorporated in the opening forms, covering the following information :-

#### **7.3.02.01. Mandatory Information to be included in the opening form :-**

- 1) Occupation
- 2) Source of funds
- 3) Monthly Income
- 4) Annual turnover
- 5) Date of Birth
- 6) Dealings with other banks
- 7) Existing credit facilities

#### **7.3.02.02. The following information may be collected by the branch (which is Optional) for better customer relationship:-**

1. Marital Status;
2. Educational Qualification;
3. Educational Qualification of spouse;
4. Details regarding children;
5. Information like -
  - a) Owns a car/two wheeler
  - b) have credit card
  - c) Have insurance policy.

### **7.3.02.03. Periodical Review of Customer Profile**

The Customer profiles incorporated in the opening forms have to be reviewed once in three years.

### **7.3.02.04. The account opening form**

For opening accounts by transfer from other branches, a new set of account opening forms along with the customer profile to be obtained.

While transferring accounts from inoperative accounts to live ledger, a new set of account opening form along with the customer profile to be obtained/ updated.

The prospective customer should not be insisted upon for the optional information. Wherever branch/office desires to collect any information about the customer for the purpose other than KYC requirement, it should not form part of the account opening form. Such information may be collected separately, purely on a voluntary basis after explaining the objective to the customer and taking customers express approval for the specific uses to which such information could be put.

The aforesaid optional information may not be insisted upon from the existing customers. The information given in the Account Opening Form other than optional information, as mentioned above, are mandatory, as such branches must obtain the same so as to comply with the KYC guidelines.

**Caution is to be exercised with regard to introduction of large number of accounts by a single introducer (either account holder or staff).**

### **7.3.02.05 CHECK LIST**

**Features to be verified and documents that may be obtained from customers**

<b>Features</b>	<b>Documents</b>
Accounts of individuals	Recent Photograph and (any one document which provides customer information to the satisfaction of the branch)
Legal name and any other names used	Passport PAN card Voter's Identity Card Driving licence Identity card (subject to the bank's satisfaction)

*Correct permanent address	Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch/office Telephone bill Bank account statement Letter from any recognized public authority Electricity bill Ration card Letter from employer (subject to satisfaction of the branch)
Accounts of companies	Certificate of incorporation and Memorandum & Articles of Association
Name of the company	Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account
Mailing address of the company	Copy of PAN allotment letter
<b>Accounts of partnership firms</b>	Registration certificate, if registered
Legal name	Partnership deed
Address	Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
Names of all partners and their addresses	Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses
Telephone numbers of the firm and partners	Telephone bill in the name of and partners
<b>Accounts of trusts &amp; foundations</b>	
Names of trustees, settlers, beneficiaries and signatories	Certificate of registration, if registered. Power of Attorney granted to transact business on its behalf
Names and addresses of the founder, the managers/directors	Any officially valid document to identify settlers, beneficiaries and

and the beneficiaries	those holding Power of Attorney founders/managers/directors' addresses
Telephone/fax numbers	Resolution of the managing body of foundation/association Telephone bill

**Customers will be classified into three risk categories namely High, Medium and Low**, based on the risk perception. The risk categorization will be reviewed periodically.

The Customer Identification Procedures are to be carried out at the following stages:

- o While establishing a banking relationship;
- o When the **bank** feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.
- o Customer identification data (including photograph/s) should be periodically updated after the account is opened. Such verification should be done atleast once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk customers.
- o Customer Identification will also be carried out in respect of non-account holders approaching **bank** for high value one-off transaction as well as any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank.

#### **7.4 Small Deposit (No Frills) Accounts:**

With a view to ensuring financial inclusion such that persons, especially those belonging to low income group both in urban and rural areas, who are not able to produce such documents required by the Cooperative/Regional Rural Bank to satisfy about their identity and address, are not denied banking services, branches may open Small Deposit (No Frills) accounts, for natural persons only, with relaxed KYC standards, as detailed in the operating guidelines. Persons desirous of opening such accounts can keep aggregate balances not exceeding Rs. 50,000/- (Rupees fifty thousand only) in all their accounts taken together and the total credit, again in all accounts taken together, should not exceed Rs. 1,00,000/- (Rupees one lac only) in a year.

If at any point, the balances in all his/her accounts with the **Bank** (taken together) exceeds Rs. 50,000/- (Rupees fifty thousand only) or total credit in all accounts taken together exceeds Rs. 1,00,000/- (Rupees one lac only) in a year, no further transactions will be permitted until full KYC procedure is completed. **Bank** would notify the customers when the balances reach Rs.

40,000/- (Rupees forty thousand only) or total credit in a year reaches Rs. 80,000/- (Rupees eighty thousand only) so that appropriate documents, for complying with full KYC requirements are submitted well in time to avoid blocking of transactions in the account.

## **7.5 Monitoring and Reporting of Transactions**

### **Monitoring of Transactions**

Ongoing monitoring is an essential element of effective KYC procedures. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

#### **7.5.01. High-risk accounts**

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

The branch/office may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions, which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

High-risk accounts have to be subjected to intensified monitoring. Bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

#### **7.5.02. Cash Transactions** (Issue of DD/TT/MT/PO,etc.)

Banks are required to issue travelers cheques, demand drafts, mail transfers and telegraphic transfers for Rs.50,000 and above only by debit to customers accounts or against cheques and not against cash.

Applicants (whether customers or not) should furnish permanent (income tax) account number (PAN) on the application for issue of travelers cheques, demand drafts, mail transfers and telegraphic transfers if the amount exceeds Rs. 50,000.

In case customer/account holders not having PAN, since their income (from all sources) falls below the income tax exemption limit, the procedures to be adopted is mentioned below.

### 7.5.03 For PAN – undernoted procedure to be followed :

Category of Customer	Procedure adopted
1. Account holders having PAN and recorded with bank	A suitable provision is available in the Draft/TT/Bankers' order/RTC application form for affixing PAN under the signature of the account holder.
2. Account holders not having PAN since their income (from all sources) falls below the Income Tax exemption limit	A declaration in Form No.60 of I.T. Rules to be obtained (form being obtained to open the new accounts from the customers not having the PAN). The declaration is to be obtained along with the application Form. The account holder should sign the declaration to be printed on the reverse of the application form.
3. Account holders not allotted PAN even though applied for it (holding acknowledgement for application) but their income is assessed for Income Tax and Assessment order issued by appropriate authority.	A declaration on Form No.60 of IT Rules be obtained. The account holder should give a suitable statement in the form. The official in-charge of the drafts business at the Branch should act diligently and satisfy himself about the genuineness of the statement.
4. Account holders who have agricultural income and is not in receipt of any other income chargeable to Income Tax	A declaration on Form No.61 of IT Rules be obtained (as this is the form permitted to open the New accounts for a person who has agricultural income and is not in receipt of any other income chargeable to Income Tax for not having the PAN). The declaration is printed on the reverse of the application form. The account holder should sign the declaration printed on the reverse of the application form.
5. Account holder whose income is neither assessed for IT nor applied for PAN and not fall under any of the category (1) to (4) above.	The account holders will be advised to obtain the PAN and his application for purchase of DD/TT/BO/RTCs for Rs.50,000/- and above be rejected politely.

Further income tax Act and Rules require obtention of PAN only in cash purchase of bank drafts/pay orders/bankers cheque aggregating Rs. 50,000/- or more during any one day from a banking company (branch).

Branches/Offices should ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the Prevention of Money Laundering (PML) Act, 2002, wherein it is stated that the Banking companies, financial institutions, interme-diaries and their officers shall not be liable to any civil proceedings against them for furnishing information under the Act.

It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, is reported to the appropriate law enforcement authority.

Branches are required to report all cash deposits and withdrawals of Rs.10 lakh and above as well as transactions of suspicious nature with full details in fortnightly statements to their respective controlling offices. The controlling offices are also required to appraise the Head office regarding transactions of suspicious nature.

#### **7.5.04. PROCESS AND PROCEDURES TO MONITOR SUSPICIOUS TRANSACTIONS**

Branches are required to record and report all transactions of suspicious nature in deposit, loan and remittance accounts etc, with full details to their controlling Offices.

#### **7.5.05 Transactions of suspicious nature**

The procedure to be followed is as under -

The Principal officer/Officer -in charge, vested with the authority to open the account, is to ensure compliance with the KYC guidelines. The employee/officer, who has interviewed the customer's to subscribe his signature for having interviewed the prospective customer and the officer, before permitting opening of the account, to satisfy that all aspects of KYC guidelines are complied with.

In cash transactions RBI/NABARD's guidelines are required to be strictly complied with and a close watch of individual/integrally connected cash withdrawals and deposit for Rs.10.00 lakh and above in deposit, cash credit or overdraft accounts and recording of the transactions in a separate register is to be done.

### **Threshold limit of transaction**

At the time of opening of the account, based on customer's profile, a threshold limit of transaction is to be determined. To begin with all transactions up to Rs. 10.00 lakh will be exempted from the purview of the scrutiny. Further; it is proposed to have a threshold limit of Rs.50000/- in case of individuals; one month turnover in the case of business enterprise (including business professionals) or Rs. 10.00 lakh wherever is lower. These limits are to be reviewed and revised on yearly basis or as requested by the customer from time to time and any transaction beyond this limit should be looked into with extra caution.

Activity monitoring to cover all accounts including existing accounts for which profile to be made over a period of time. Branch Managers should use reasonable judgment in determining the suspiciousness of the transaction and the accounts wherein the suspicious transactions were found are to be closely monitored at the branches, so that the documentary evidence upon which a suspicion is aroused is not lost.

A courteous approach in the process is very essential to take care that the customers are not driven away from the **Bank**.

### **7.5.06. Reporting system for high value cash/suspicious transaction**

#### **7.5.07. Cash transaction of Rs. 10.00 lakh and above**

Branches are required to record and report all individual/integrally connected cash deposits and withdrawals of Rs. 10.00 lakh and above in deposits, cash credit and overdraft accounts etc, at fortnightly intervals to the respective controlling Offices.

#### **7.5.08 Suspicious Transactions**

To observe four eyes concept in reporting suspicious transactions at branch level, first dealing officer at the branch will report to the Branch Manager (BM), who will get himself satisfied about existence of a suspicious activity/nature and then report to the controlling office. Further course of action is to be recommended by the controlling officer in consultation with Law Department to H.O. The designated officer at H.O has to take up the matter with appropriate law enforcing authorities designated under the relevant laws governing such activities.

The Controlling Authority during their visit/surprise inspection to Branch, have to verify the account opening forms/transactions recorded in the register for the purpose at random.

#### **7.5.09 Terrorist finance**

In case the name of any banned organization is noticed as payee/endorsee/applicant, the first dealing officer shall report the same to the

Principal Officer. Reporting of such transactions as and when detected is to be done as under:

<i>Reporting by</i>	<i>Reporting to</i>
1. Branch	1. Controlling office
2. Controlling office	2. Principal Officer(PO). H.O.
3 .PO. H.O	3.RBI (till RBI/Govt. Identifies appropriate authority)

Transactions which are of suspicious nature and required to be reported to FIU-IND are given in Annexure I.

Monitoring of transactions will be conducted taking into consideration the risk profile of the account. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer will be subjected to detailed scrutiny.

System supported monitoring of transactions will be done by the AML team under the Principal Officer, based on alerts thrown up by the AML software acquired/to be acquired by the Cooperative/Regional Rural Bank and on the basis of feedback/inputs from the controlling offices and respective relationship points. Simultaneously, however, relationship points will maintain oversight over the transactions with a view to identifying suspicious transactions and bringing them to the notice of the Principal Officer.

After due diligence at the appropriate level in the Bank, transactions of suspicious nature and/or any other type of transaction notified under PMLA will be reported by the Principal Officer to Financial Intelligence Unit – India (**FIU-IND**), the appropriate authority. A record of such transactions will be preserved and maintained for the period as prescribed in PMLA.

Transactions in the accounts will also be monitored with a view to timely submitting, the Cash Transaction Report (**CTR**) in respect of cash transactions of Rs. 10,00,000/- (Rupees ten lakh only) and above undertaken in an account either singly or in an integrally connected manner.

All cash transactions, where forged or counterfeit Indian currency notes have been used, shall also be reported immediately by the branches, by way of Counterfeit Currency Reports (**CCRs**) to the Principal Officer, through proper channel, for onward reporting to FIU-IND.

### **7.5.10 Closure of Accounts**

Where the appropriate KYC measures could not be applied due to non-furnishing of information and/or non-cooperation by the customer, the account can be considered for closure or terminating the banking/ business relationship. Before exercising this option, all efforts will be made to obtain the desired information and, in the event of failure, due notice, will be given to the customer explaining the reasons for taking such a decision. In all cases, the controlling authority at the respective controlling office/Head office shall be the competent authority to permit closure of such accounts.

### **7.6 Risk Management**

The bank has put in place an effective KYC programme in place by establishing appropriate procedures and ensuring their effective implementation covering proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has also been explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively.

The nature and extent of due diligence will depend on the risk perceived by the branch/bank. However, while preparing customer profile branches should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

Bank's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. It would be ensured that the audit machinery is staffed adequately with individuals who are well versed in such policies and procedures.

Internal Inspectors should specifically check and verify the application of KYC procedures at the branches/offices and comment on the lapses observed in this regard. The compliance in this regard may be put up before the Audit Committee of the Board by HO (Inspection) on quarterly intervals.

While the Cooperative/Regional Rural Bank has yet to adopt a risk-based approach to the implementation of this Policy, it is necessary to establish appropriate framework covering proper management oversight, systems, controls and other related matters.

Bank's Internal Audit of compliance with KYC/AML Policy will provide an independent evaluation of the same including legal and regulatory requirements.

The Principal Officer designated by the Bank in this regard will have overall responsibility for maintaining oversight and coordinating with various

functionaries in the implementation of **KYC/AML/CFT policy**. However, primary responsibility of ensuring implementation of **KYC/AML/CFT Policy** and related guidelines will be vested with the respective controlling Office. Suitable checks and balances in this regard will be put in place at the time of introducing new products/procedures as also at the time of review of existing products/ procedures for overall risk and compliance management. For this purpose, each controlling office will designate an official as Money Laundering Reporting Officer (**MLRO**) who would ensure proper implementation and reporting, as per provisions of this **Policy**, to the Principal Officer.

#### **8. Employee Training**

All employee training programmes, of 6 days' duration or more, will have a module on KYC Standards/AML/CFT Measures so that members of the staff are adequately trained in **KYC/AML/CFT** procedures.

Records to be kept of all formal training conducted. These records have to include the names and other relevant details, dates and locations of the training.

#### **9. Recruitment/Hiring of Employees**

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse channels of the Cooperative/Regional Rural **Bank**. The **bank** will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel.

#### **10. Customer Education**

The Cooperative/Regional Rural **Bank** recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose. The front desk staff would be specially trained to educate the customers regarding the objectives of the KYC programme.

#### **11. Introduction of New technologies**

**The bank** will pay special attention to the money laundering threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering activities. The bank will ensure that appropriate KYC procedures are duly applied to the customers using new technology driven products.

#### **12. KYC for the existing accounts**

While the KYC guidelines will apply to all new customers, the same would be applied to the existing customers on the basis of materiality and risk. However, transactions in existing accounts would be continuously monitored for any unusual pattern in the operation of the accounts. On the basis of

materiality and risk the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural /legal person and those of the `beneficial owners`. Similarly, the Cooperative/Regional Rural Bank will also ensure that term / recurring deposit accounts are subject to revised KYC procedures at the time of renewal of the deposits on the basis of materiality and risk.

### **13. Record Keeping**

Branches/offices should prepare and maintain documentation on their customer relationships and transactions to meet the requirements of relevant laws and regulations, to enable any transaction effected through them to be reconstructed.

### **14. Retention of Records**

In terms of the Banking Regulation Act, records such as Account Opening Forms, vouchers, ledgers, registers etc., pertaining to Banking Transactions for specified periods are required to be maintained. In addition, the following documents in respect of accounts, which have been reported for suspicious activities, are required to be retained at the end of business relationship with the customer, which in any case shall not be less than 10 years.

1. Customer Profiles
2. Reports made to government authorities concerning suspicious customer activities relating to possible money laundering or other criminal conduct together with supporting documentation.
3. Records of all formal anti money laundering training conducted which include the names and business units of attendees and dates and locations of the training; and
4. Any other document required to be retained under applicable money laundering laws/regulations.

All financial transactions records are to be retained at least for 10 years after the transaction has taken place and to be made available for scrutiny of Law enforcing agencies, Audit functionaries as well as Regulators as and when required.

### **15. Correspondent Banking**

This policy will apply to our dealings with correspondent banks. For correspondent banking relationship an appropriate due diligence procedure will be laid down keeping in view KYC standards existing in the country where the correspondent bank is located and the track record of the correspondent bank in the fight against money laundering and terrorist financing.

## **16. Miscellaneous:**

- Information collected from the customers for KYC compliance should be relevant to the perceived risk, not intrusive and should be treated as confidential. The same is not to be used/divulged for cross selling or any other such purpose.
- Any remittance of funds by way of demand drafts, mail/telegraphic transfer or any other mode like RTGS/ NEFT and issue of payment orders for value Rs.50,000 and above is effected only by debit to customer's account or against cheques/drafts and not against cash.
- Provisions of Foreign Contribution (Regulation) Act, 1976, as amended from time to time, wherever applicable, should be strictly adhered to.

## **17. Principal Officer**

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

- Overall monitoring of the implementation of the Bank's **KYC/AML/CFT policy**.
- Monitoring and reporting of transactions, and sharing of information, as required under the law.
- Interaction with MLROs at the controlling offices for ensuring full compliance with the **Policy**
- Timely submission of Cash Transaction Reports (CTRs), Suspicious Transaction Reports (STRs) and Counterfeit Currency Reports (CCRs) to FIU-IND
- 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.
- Ensuring submission of periodical reports to the Top Management/ Board.

## **18. Review of the Policy**

The **Policy** will be reviewed as and when considered necessary by the Board. An independent evaluation of KYC guidelines for identifying high value transactions is required to be carried out by Concurrent/ Internal Auditors. They are required to comment on the effectiveness of measures taken by

branch level implementation of KYC guidelines and prevention of Money-Laundering at branches/ offices.

**19. Duties and Responsibilities and Accountability**

The illustrative areas of duties and responsibilities of various categories of staff together with their accountability are given in Annexure II.



**Transaction of suspicious nature**

**(I) Transactions not consistent with customer's business**

1. Frequent withdrawals in cash by corporate customers, instead of cheque transactions without giving cogent reasons.
2. Customers insisting on cash payment of cheques drawn in the name of the firm without routing through their account, quoting reason for pressing payment of outstanding dues.
3. High value deposits routed through newly opened accounts and gradual cash withdrawals leaving small balances.
4. A single substantial cash deposit composed of many high denomination notes.
5. Instruments with multiple endorsements.
6. Accounts where large volume of credits through DD/TT/BC whereas the nature of business does not justify such credits.
7. Frequent exchange of small denomination notes for large denomination notes and vice versa in large quantities.
8. Frequent credits in cash into the account by person other than the account holder or his authorized representative.

**(II) Attempt to avoid reporting/ circumventing prescribed guidelines**

Frequent issue of demand drafts/banker's cheques / telegraphic transfers for sums deposited in cash just below threshold limit of Rs.50,000/- thereby not routing the transaction through the account.

Intentional splitting of transactions into small amounts to avoid reporting of transaction which may become necessary in case the threshold limit is crossed.

Requesting **Bank** to open multiple accounts with a view to circumvent reporting by the **Bank** as per existing regulations.

Frequent opening and closing of accounts in short duration of time with a view to avoiding reporting of transactions involved as per existing regulations.

**(iii) Unusual activities**

1. Opening of account at places away from place of work/residence of the individual/firm.
2. Frequent operations in safe deposit lockers followed by cash deposits especially deposits just under the threshold levels.
3. Frequent deposit of large sums of money bearing labels of other banks into the accounts.
4. Request for closure of newly opened accounts where high value transactions have been routed through them and funds withdrawn immediately.

(iv) Customers who provide insufficient or suspicious information

1. Reluctance of the customer/corporate to furnish details about their activities or providing financial statements.
2. A customer who has no record of past or present employment but makes frequent large transactions through the account.
3. Letter of thanks sent to the customer/introducer returned undelivered.

(v) Certain **Bank** employees arousing suspicion

1. Unexplained shortages of significant amount of Bank's funds reported on account of the same employee(s).
2. Reluctance to take job rotation/routine transfer.
3. Employee does not avail leave/vacation.
4. Negligence of employee's willful blindness is reported repeatedly.
5. Life-style of the employee inconsistent with the known sources of income.
6. Frequently exceeding the discretionary power and allowing excess drawings to borrowers without proper justification/reporting to appropriate authority for control.
7. Request for frequent DD purchases of high value instruments by staff members.

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

- Large cash transactions.
- Multiple accounts under the same name.

- Frequently converting large amounts of currency from small to large denomination notes.
- Placing funds in term deposits and using them as security for more loans.
- Large deposits immediately followed by wire transfers.
- Sudden surge in activity level.
- Same funds being moved repeatedly among several accounts.
- Multiple deposits of money orders, Banker's cheques, drafts of third parties etc.
- Transactions inconsistent with the purpose of the account.
- Maintaining a low or overdrawn balance with high activity.

#### Note

1. The above list is illustrative and not exhaustive. The Principal Officer of the Branch/Office where suspicious activity/transaction is reported should verify the report depending upon the circumstances of the activity/ transaction reported and satisfy himself whether the activity/ transaction is to be reported as a suspicious activity/ transaction or is to be treated as a bonafide one. Care should be taken that the customers with bonafide transactions are not inconvenienced.

2. Activity monitoring should cover all accounts including existing accounts for which profiles have not been made.

### **Indicators for suspicious transactions**

Suspicion of proceeds of crime  
Match of customer details with known criminals or persons with suspicious background  
Match with UN list – IS IT BEING DONE IN SCBs/DCCBs/RRBs??  
Customer has been the subject of a law enforcement inquiry  
Customer who conducts transactions in a pattern consistent with criminal proceeds  
Lottery scam or recruitment scam  
Multi-level marketing  
Transaction from high risk or sensitive area  
Unusual or complex transaction  
Transaction is unnecessarily complex  
Unusual single or aggregate transfers  
Transaction is inconsistent with customer profile  
Routing of transfer through multiple locations or accounts or unexplained transfers between accounts  
“U-Turn” Transactions  
Structuring - transactions split to evade reporting  
Unexplained activity in dormant accounts  
Suspicious use of ATM card  
Doubtful source of payment for credit card purchases

### **No economic rationale or bonafide purpose**

Volume or frequency of transactions has no economic rationale  
Use of agents or associates to disguise the beneficial owner  
Common Unique IDs used by multiple customers  
Common address/telephone used by multiple unrelated customers  
Multiple cash transactions in a single day  
Transactions with countries known for secret banking practices  
Transactions inconsistent with customer’s profile  
Maintaining multiple accounts without explanation  
Unexplained cash deposits in bank account  
Frequent cash transactions just under the reporting threshold  
Multiple cash transactions in multiple accounts  
Cash deposits followed by issue of instruments  
Suspicious cash withdrawals from bank account  
High value cheque deposits followed by immediate cash withdrawals

### **Non Financial Indicators**

Usage of Lockers

### **Behavioural Indicators**

Customer is hurried, nervous or evasive  
Customer has no or little knowledge about transaction  
Customer is accompanied by unrelated individuals.

Reluctance to meet in person, representing through power of attorney  
Customer aborts transaction after being informed that identification information will be required  
Reluctance to provide original ID  
Customer makes inquiries or tries to convince staff to avoid reporting  
Providing different identifications or details (such as phone or address) on different occasions in an attempt to avoid linking of transaction.

### **Knowledge Indicators**

Customer tries to convince staff not to complete the formalities

Customer thoroughly aware of legal position on suspicious transaction reporting.

Customer seems very conversant with money laundering or terrorist activity financing issues.

Customer is quick to volunteer that funds are clean or not being laundered.

### **Identity indicators**

Customer doubtful or vague information given.

Customer gives false identification or identification that appears to be counterfeited, altered or inaccurate.

Instead of his own some other identification is submitted by Customer.

All Identity documents presented are not verifiable i.e. Foreign documents etc.

All identification documents appear to be recently acquired.

Identity matches with known 'hot/watch lists'

### **Transactions indicators**

Frequent cash transactions in large amounts which is not normally done by the customer.

Small denominations frequently changed for large ones.

Dirty/smelly notes deposited.

Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold .

Frequent purchase of travellers cheques, DDs, etc. with cash when this appears to be outside of normal activity for the client.

### **Accounts Indicators**

A long distance customer opening an account/s.

Account/s opened with names closer to established industrial houses/ groups.

Intra bank transfer of funds - accumulated into one account for foreign remittance.

Opening of several accounts simultaneously, some of which remain dormant for long periods.

A third party appears to be using the account of customer.

Customer frequently using different locations other than the place of account opening to deposit funds.

### **Activity in account**

Account activity inconsistent with nature of business.

Transaction involves NGOs or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the NGO or charitable organization and the other parties in the transaction.

Transaction is unnecessarily complex.

### **Recent amendments in Act/ Rules**

#### **Recent changes Act/Rues**

- Concept of Beneficial ownership and definition now given in rules;
- KYC for occasional customers;
- Transactions above Rs. 10 lakhs involving NPOs;
- KYC/AML policy not to be submitted to FIU;
- Attempted transaction included in definition of Suspicious transaction;
- Retention of all records for a period of 10 years;
- Furnishing of information to be kept confidential;
- Records to contain all necessary information that allows reconstruction of transaction;

**Annexure II**

**DUTIES/ RESPONSIBILITIES AND ACCOUNTABILITY**

**The importance of KYC guidelines to the employees**

The **Bank** employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff and management shall not provide advice or other assistance to individuals who are indulging in money laundering activities. The chain of duties and responsibilities at branches/ controlling offices and accountability are as under and non-compliance of the duties and responsibilities arising out of KYC guidelines will lead to fixation of accountability. Dereliction of duty and avoidance of knowledge will lead to examination of staff accountability.

***Personnel***

***Duties/Responsibilities***

Officer in Charge of accounts/  
Officer vested with the  
authority to open new accounts

To interview the potential customer  
To verify the introductory  
reference/ customer profile

To arrive at threshold limits for each  
account (new as well as existing) and  
to exercise due diligence in identifying  
suspicious transactions.

To ensure against opening of accounts  
in the names of terrorist/ banned  
organizations  
To adhere to the provisions of Foreign  
Contribution Regulatory Act 1976.

To comply with the guidelines issued  
by the **bank** from time to time in  
respect of opening and conduct of  
account.

Principal Officer

To scrutinize and satisfy himself/  
herself the information furnished in  
the account opening form/ customer  
profile/threshold limit are in strict  
compliance with KYC guidelines before  
authorizing opening of account.

To certify in the Statement /Register  
regarding compliance with KYC  
guidelines and report suspicious  
transactions to appropriate authority.

Concurrent Auditor

To verify and record his comments on the effectiveness of measures taken by branches/level of implementation of KYC guidelines

Controlling Authority

Prompt reporting of information regarding suspicious transactions to the law enforcing authority concerned in consultation with Principal Officer at Head Office.

@@@@@