POLICY Guidelines on KNOW YOUR CUSTOMER (KYC)
ANTI MONEY LAUNDERING (AML)
And COMBATING OF FINANCING OF TERRORISM (CFT) MEASURES

1. Preamble

In terms of the guidelines, issued by the Reserve Bank of India (RBI) during 2004, Banks were required to put in place a comprehensive policy framework covering the KYC Standards and AML Measures. The guidelines also took into account the recommendations made by the Financial Action Task Force (FATF) on AML measures and CFT measures as well as the Basel Committee on Banking Supervision document on Customer Due Diligence (COD) measures. Accordingly a Policy Document on KYC and AML guidelines was formulated and adopted by the Banks in India after approval by their respective Boards. Consequent upon amalgamation of erstwhile Aryavart Kshetriya Gramin Bank and Shreyas Gramin Bank vide GOI Notification F.no.7/9/2011-RRB (UP-I) dated 01.04.2013 into a single amalgamated entity 'Gramin Bank Of Aryavart', the Board of Bank adopted **KNOW YOUR CUSTOMER (KYC**) and **ANTI MONEY LAUNDERING (AML) MEASURES** in its 1st meeting held on 28.05.2013. Consequent upon the PML Act coming into force, the Bank's obligations there under have also been put in place and compliance of the same are being adhered to.

This Policy document aims at consolidating all instructions/guidelines issued from time to time on KYC Standards, AML Measures, CFT Measures and Bank's obligations under the PML Act, 2002.

2. Objective

The objective of the Policy is:

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

b) To enable the Bank to know/understand the customers and their financial dealings better thereby helping us to manage the risks prudentially.

c) To put in place a proper control mechanism for detecting and reporting of suspicious transactions in accordance with the statutory and regulatory provisions.

d) To ensure that all the provisions of Prevention of Money Laundering Act, 2002 and the Rules made there under and all subsequent amendments thereof are complied with.

3. Scope

This policy is applicable to all branches / offices of the bank. Branches should keep in mind that the information collected for the purpose of opening of account is to be kept as confidential and details thereof are not to be divulged for cross-selling or any other purposes. Information sought should be relevant to the perceived risk and should not be intrusive. Any other information from the customer should be sought separately with his/her consent and after opening the account.

4. Definition of Money Laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 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 the offence of money laundering".

The essential ingredients of money laundering are:

- A crime has been committed
- There are proceeds of or gains from the crime; and
- There is a transaction in respect of the proceeds of the gain

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 policy document, the term 'money laundering' shall include financial transactions where the end use of funds is for terrorist financing irrespective of the source of funds.

The following situations though not exhaustive may indicate money laundering and can help the Bank in recognizing ways launderers may approach them;

- Activity Not Consistent with the Customer's Business
- Unusual Characteristics of Activities
- Attempts to Avoid Reporting or Record – Keeping Requirements
- Certain Funds Transfer Activities
- A Customer Who Provides insufficient or Suspicious Information
- Extraordinary transactions under employee accounts.
-

5. Obligations under prevention of Money Laundering (PML) Act 2002:

Section-12 of PML Act 2002 places certain obligations on every banking company, financial institution and intermediary, which include:

(i) Appointment of a Principal Officer;

(ii) Maintaining record of prescribed transactions;

(iii) Furnishing information of prescribed transactions to the specified authority;

(iv) Verifying and maintaining records of the identity of its clients;

(v) Preserving records in respect of [ii] and [iii] above for a period of at least ten years from the date of each such transaction between the Bank and the client;

(vi) Preserving records in respect of [iv] above for a period of at least ten years after the business relationship is ended.

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

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.

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:-

“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.”

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.

6. Money Laundering - Risk Perception

Bank is exposed to the following risks which arise out of Money Laundering activities:

- **Reputation Risk**

  Risk of loss due to severe impact on bank's reputation

- **Compliance Risk**

  Risk of loss due to failure to comply with key regulations governing the Bank's operations.

- **Operational Risk**

  Risk of loss -resulting from inadequate or failed internal processes, people and systems, or from external events.

- **Legal Risk**

  Risk of loss due to any legal action the Bank or its staff may face due to failure to comply with the law.

Risk Perception in respect of Customer:

For categorizing a customer as low risk, medium risk and high risk, the parameters considered are location of customer and his client, mode of payments, nature of activity, volume of turnover and social and financial status.

A. Low Risk Customers (Level 1 customers):

- Salaried employees
- People belonging to lower economic strata of the society
- Government Departments
- Government owned companies
- Regulatory and Statutory bodies, etc.

For the above category, the KYC requirements of proper introduction, identification and verification of proof of address would suffice.

B. Medium Risk Customers (Level 2 customers):

- High net worth individuals
- Non-Resident customers

For this category, higher due diligence is required which includes customer’s background, nature and location of activity, country of origin, source of funds and his/her client profile, etc. besides proper introduction and identification.

C. High Risk Customers (Level 3 customers):

- Trusts, charities, NGOs and organizations receiving donations
- Companies having close family shareholding or beneficial ownership
- Firms with ‘sleeping partners’
- Accounts under Foreign Contribution Regulation Act

- Politically exposed persons (PEPs) of foreign origin
- Those with dubious reputation as per public information available
- Accounts of non- face- to face customers, etc.
- Non-Resident Accounts
- High Net worth Individuals

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper introduction and identification. Bank should subject such accounts to enhanced monitoring on an ongoing basis.

(The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Branch/Office.)

Branches / Offices should prepare a profile for each new customer based on risk categorization. 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. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile Branches/Offices 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 is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

For the purpose of risk categorization, 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 categorized 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 and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that 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 should 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. Branches/Offices should apply enhanced due diligence measures 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. Examples of customers requiring higher due diligence include (a) non resident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with ' sleeping partners '; (f) politically exposed persons (PEPs) of foreign origin; (g) non-face to face customers and (h) those with dubious reputation as per public information available etc. However, only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer.

It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

7. Definition of Customer

For the purpose of this policy, a 'Customer' is defined as:

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

Regional Offices / branches should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. It should be ensured that the information sought from the customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued in this regard, Any other information from the customer should besought separately with his / her consent after opening the account.

(The aforesaid definition has a broader implication than the conventional meaning of Customer)

8. The Financial Action Task Force (FATF):

The Financial Action Task Force (FATF) defines Money Laundering as the processing of the criminal proceeds in order to disguise their illegal origin.

Under The Prevention of Money Laundering Act, 2002, the offence of money laundering shall be punishable with rigorous imprisonment for a term not less than 3 years and may extend to 7 Years. Further in respect of Money Laundering through offences under Narcotic Drugs and Psychotropic Substance, the punishment can be up to 10 years instead of 7 years.

9. 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

10. "Know Your Customer" Standards:

The objective of KYC guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for money laundering activities. The four main pillars on which the KYC norms of the Bank rests are:

A. Customer Acceptance Policy (CAP)

B. Customer Identification Procedures (CIP)

C. Monitoring of Transactions (MT) and

D. Risk Management (RM)

A. 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:

1. No account is to be opened in anonymous or fictitious / benami name(s)/entity(ies)
2. Accept customers only after verifying their identity, as laid down in Customer Identification Procedures. 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.
3. 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 categorization.
4. Documentation requirements and other information to be collected, as per PMLA and RBI/NABARD guidelines/instructions, to be complied with
5. 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
6. 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.
7. 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.
8. 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.
9. 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.

(i) Introduction not Mandatory for opening accounts:

Before implementation of the system of document –based verification of identity, as laid down in PML Act/Rules, introduction from an existing customer of the bank was considered necessary for opening

of Bank accounts. Since introduction s not necessary for opening of accounts under PML Act and Rules or Reserve Bank extant KYC instructions, banks should not insist on introduction for opening bank accounts of customers. In view of provisions for 'Small Accounts' being included in PML Rules, the extant instructions for opening of 'Small Accounts' with introduction stand withdrawn.

In respect of all newly opened accounts, a Thanks Giving letter should be sent to the new account holder. This would while earning the goodwill of the customer also serves as a confirmation of residential proof of the customer. If the Thanks Giving Letter so sent is returned undelivered the branch should immediately take appropriate action to safeguard the interest of the bank.

This is equally applicable in case of conversion of individual deposit account to joint accounts also.

Opening a new account should be authorized only by the Branch Manager/Officer In charge of Branch subject to fulfillment of other conditions.

(ii) Precautions to be exercised in case of Joint accounts

The maximum number of persons for joint account is restricted to FOUR and Pension accounts can not be opened jointly.

The mode of operation should be noted in the Computer System and the specimen signature card. This note in the Computer System and the specimen signature card should be checked and initialed by the Supervisor.

Specimen signatures of each of the joint depositors should be obtained on separate specimen signature cards.

Transfer of accounts from one branch to another branch can not be done at the request of any one of the joint account holders.

Branch Manager / Officer should keep a vigil over the transactions in joint accounts involving huge amounts. Transactions should generally have a bearing with the occupation and or line of business of the account holders. In case of any doubt necessary enquiries be made with the account holders. While accepting the cheque for collection, it is to be ensured that the name mentioned in pay-in-slip and name of the beneficiary of the instrument are same.

Current Account with non-consortium banks

In terms of extant guidelines of lending under consortium, a bank which is not member of a consortium/syndicate, shall not open current account or extend any banking facility without the concurrence of the consortium/syndicate. This should be scrupulously complied with.

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 intermediary. 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.

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.

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.

Accounts under Foreign Contribution Regulation Act, 1976 (FCRA)

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.

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 identity 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.

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

Individuals/Organizations who can not receive foreign contributions

Foreign contributions can not be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employees of any corporation member of any legislature, political party or Office bearer thereof.

Individuals/Organizations who can receive foreign contributions

An association having a definite cultural, economic, educational, religious or social programme can receive foreign contribution after it obtains the prior permission of the Central Government or gets itself registered with the Central Government.

iii. Profile based on categorization:

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 branch 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.

B. Customer Identification Procedure:

(i) Need for photographs and address confirmation:-

Pass port size /stamp size photograph of the depositors should be obtained in case of all Current Accounts, SB accounts and Term Deposits.

In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public/private limited companies, HUF, trusts, etc., and those of minors, photographs of the authorized signatories should be obtained. Photographs of the student account holders should be attested by the school authorities.

In case of change in the authorized signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/organizations. Photographs should be obtained in case of NRI accounts also.

Where the accounts are operated by letters of authority, photographs of the authority holders should be obtained, duly attested by the depositors.

It has been observed that some close relatives, e.g. wife, son, daughter and daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some Branches as the utility bills required for address verification are not in their name. It is clarified, that in such cases, Branches can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Branches can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, Branches should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers. Branches should introduce a system of periodical updation of KYC customer identification data (including photograph/s) after the account is opened. Full KYC exercise will be to be done at least every two years for high risk individuals and entities and it will be required to be done at least every ten years for low risk and at least every eight

years for medium risk individuals and entities. Positive confirmation (obtaining KYC related updates through e-mail/letter/telephonic conversation/forms/interviews/visits, etc.), will be required to be completed at least every two years for medium risk and at least every three years for low risk individuals and entities. Fresh photographs will be required to be obtained from minor customer on becoming major.

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 branch or on the basis of documents provided by the customer.

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.

Existing Accounts and Small Accounts with introduction:

The provisions for opening of bank accounts with restrictions on total credits and outstanding balance, with introduction from an existing account holder or other evidence of identity and address to the satisfaction of the bank, were made to help persons who were not able to provide'Officialy valid documents' for opening accounts.In view of provisions for small accounts being included in the PML Rules, the extant instructions for opening of 'Accounts with Introduction' stand withdrawn and Banks are required to complete KYC norms in all existing small accounts and other accounts in which KYC norms have not been completed earlier at the time of opening of account.

VERIFICATION OF RECORDS OF IDENTITY OF CLIENT:

1. Every Banking Company, financial institution and intermediary, as the case may be shall-

a) At the time of commencement of an account - based relationship, identity its clients, verify their identity and obtain information on the purpose and intended nature of business relationship, and

b) In all other cases, verify identity while carrying out:

   i. Transaction of an amount equal to or exceeding Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, or

   ii. Any international money transfer operations.

1 (A). Every Banking Company, financial institution and intermediary, as the case may be shall identify the beneficial owner and take all reasonable steps to verify his identity.

1 (B). Every Banking Company, financial institution and intermediary, as the case may be shall exercise ongoing due diligence with respect to the business relationships with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

1 (C). No Banking company Financial Institution or intermediary, as the case may be, shall keep any anonymous account or account in fictitious names.

2. Where the client is an individual, he shall for the purpose of above Para N. ii – (1), submit to the banking company, financial institutions and intermediary, as the case may be, one certified copy of an "Officially valid document" containing details of his identity and address, one recent photograph and such other documents including in respect of the nature of the business and Financial Status of the client as may be required by the banking company or the Financial Institution or the intermediary, as the case may be:

   Provided that photograph need not be submitted by a client falling under clause (B) of sub-rule (1) of para ii.

3. Where the client is a company, it shall for the purpose of above sub-rule No. 1 of para ii, submitted to the banking company or Financial Institution or intermediary, as the case may be, certified copies of the following documents.
   i. Certificate of incorporation;
   ii. Memorandum of articles of associations;
   iii. A resolution from the Board of Directors and Power of Attorney granted to its Managers, Officers or employees to transact on its behalf; and
   iv. An officially valid document in respect of Managers, Officers or employees holding an Attorney to transact on its behalf.

4. Where the client is a partnership firm, it shall for the purpose of sub-rule (1) of Para ii, submit to the banking company, or the Financial Institutions, or the intermediary certified copies of the following documents:
   i. Registration certificate;
   ii. Partnership deed; and
   iii. An officially valid document in respect of the person holding an Attorney to transact on its behalf

5. Where the client is a trust , it shall, for the purpose of above sub-rule (1) of para ii, submit to the banking company, or the Financial Institutions, or the intermediary certified copies of the following documents:
   i. Registration Certificate;
   ii. Trust deed; and
   iii. An officially valid document in respect of the person holding an Attorney to transact on its behalf

6. Where the client is an incorporated association or a body of individuals, it shall submit to the banking company, or the Financial Institutions, or the intermediary copies of the following documents:
   I. Resolution of the managing body of such association or body of individuals;

II. Power of attorney granted to him to transact on its behalf;

III. An officially valid document in respect of the person holding an Attorney to transact on its behalf; and

IV. Such information as may be required by the Banking Company or the Financial Institutions, or the intermediary to collectively establish the legal existence of such an association or body of individuals.

6 (A) where the client is the judicial person, the banking company, Financial Institution or intermediary, as the case may be, shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

Documents that are normally relied upon as proof of customers' address:-

At the time of opening of new account, correctness of address of customer should be ensured.

Customer Identification Procedure

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

Features	Documents
Accounts of individuals - Legal name and any other names used	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (vii) Aadhaar Letter issued by UIDAI and (viii) NREGA Job card
-Correct permanent address	(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) (any one document which provides customer information to the satisfaction of the bank will suffice) (vii)A rent agreement indicating the address of the customer duly registered with the state government or similar registration authority

Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms - Legal name – Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers /directors and the beneficiaries - Telephone / fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv)Resolution of the managing body of the foundation/association (v) Telephone bill

A Photostat copy of the above proof should be filed along with the account opening form.

In case of need, Branch Manager can depute an official to visit the account holder at the given address to satisfy about the genuineness of the address.

To ease the burden on the prospective customers in complying with KYC requirements for opening new accounts, it has now been decided by the RBI that:

a) If the address of the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof for both identity and address.

b) If the address indicated on the document submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address should be obtained.

c) KYC verification of all the members of SHG need not to be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linkage of SHGs, it is clarified that since KYC would have already

verified while opening the savings bank account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary.

d) For opening of new accounts of foreign students in India, proof of identity on the basis of Pass-Port and photograph attested by educational institution may be taken at the time of opening of account. Address proof will be required with in 30 days from the opening of account

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.

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 :-

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

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.

Periodical Updation of KYC

Banks are required to do periodical updation of customer identification data (including photograph/s)

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

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, account opening form along with the customer profile is to be 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).

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.

C. 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. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Branch 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. Every 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. Branches should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months.

(i) 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.

(ii) 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.

(iii) Intelligent and close watch over newly opened accounts :-

A close and intelligent watch over the newly opened accounts, especially during the first six months is to be exercised in allowing operations therein, particularly, those involving huge deposits and withdrawals.

Branches should be very cautious if cheques / drafts for large amounts are lodged for collection immediately after opening the account and the depositor is anxious to withdraw the proceeds of the cheques/drafts. Transactions disproportionately large to the occupation or line of business of the account holder may be enquired from them.

(iv) Issue and payment of demand drafts for Rs.50,000 & above:-

Very often it is observed that banking channels are misused for violation of fiscal laws and evasion of taxes. To curb this tendency, DDs for Rs.50,000/- and above should be issued only by debit to the customers account or against cheques or other instruments tendered by the purchaser and not against cash payment.

Wherever requests for issue of multiple drafts favouring the same beneficiary with total amount of such drafts exceeding Rs.50,000/- are received with latent intention of violating fiscal laws and evasion of tax, the guidelines should be made applicable in letter and spirit.

Payment of DDs for Rs.50,000/- and above should be made through banking channels and not in cash. Branches /offices have to note that the same for strict compliance.

(v) Provisions of Income Tax Act,1961:-

As per Section 269T of the Income Tax 1961, no branch of a banking company or a cooperative bank and no other company or co-operative society and no firm or other person shall repay any loan or deposit made with it otherwise than by an account payee cheque or account payee bank draft drawn in the name of the person who has made the loan or deposit if the amount of the loan or deposit together with interest, if any, payable thereon is **twenty thousand rupees or more**.

(vi) Information to CBDT – " for investigation- Compulsory quoting of PAN ":-

Information in respect of payment in cash for purchase of bank draft or a banker's cheque would be called for from banks for amount exceeding Rs. 1 lakh by CBDT and the same needs to be provided.

(vii) Monitoring of cash withdrawal and deposits of Rs.10 lakhs and above in deposit accounts, Cash Credit Account, OD account etc.:-

The RBI has advised banks to introduce a system of closely monitoring cash deposits and withdrawals for Rs.10 lakhs and above in deposit accounts and also in all other accounts like cash credit/overdraft, etc. It was also indicated therein that the branches should maintain a separate register to record details of individual cash deposits and withdrawals for Rs.10 lakhs and above.

To comply with RBI guidelines, all our branches are requested to record the Cash deposits and cash withdrawals for Rs.10 lacs and above in deposit accounts and also in all other accounts like overdraft, cash credit etc., in a register. A monthly statement furnishing the details of transactions so recorded, to be submitted to Head office.

While furnishing the information, branches are required to undertake due diligence in respect of proper identification of customers as well as unusual transactions in the accounts.

(viii) Monitoring Large Value Transactions:-

In addition to regular monitoring of operations in cash credit / overdraft accounts, a scrutiny of each drawal of Rs.25 lacs and above is to be made in case of all large borrowal accounts and ensure before allowing such drawal that the amount is drawn for purposes for which credit facility has been sanctioned.

(ix) Follow up and review of high value transactions:-

The Head Office should follow-up, receive and scrutinize the statements. In case transactions prima facie appear to be dubious or giving rise to suspicion, further details may be obtained from the branch by deputing an official.

The Head office shall, after scrutiny of the statement, place a Review Note before the Chairman of the Bank.

A certificate on calendar quarter shall be placed before the Chairman of the Bank. The Certificate shall confirm having: -

1. Received all the fortnightly statements fallen due during the quarter.
2. Scrutinized the same;
3. Taken necessary steps as advised herein before; and
4. Submitted Review Note wherever applicable.

Such Certificate shall be placed within 45 days from the respective calendar quarter.

(x) Reporting irregular practices in any operational areas including frauds and malpractices by an employee to higher authorities (Whistle blowing):

Employees who come across any irregular practices indulged at branches / offices are requested to report the matter immediately to any of the following authorities.

- Vigilance Officer, Vigilance Department, HO.
- Senior Manager, Overseeing staff matters, HO.

(xi) Accounts under Foreign Contribution Regulation Act,1976 FCRA) :

- **Compliance Requirements:** Crediting of foreign inward remittances to the beneficiaries account will have to be done only after ensuring that such individuals / organizations have registered with the Ministry of Home affairs, GOI and the account maintained by the branch is the account nominated by the beneficiary in its registration with the Govt. of India.

- **Reporting Requirements:** A quarterly statement as per the prescribed format should be submitted to the Ministry of Home affairs, Government of India, furnishing the full details of the remittances received into the account.

The above requirements are to be strictly adhered to. Any violations/deviations from the provisions of **Foreign Contribution Regulation Act, 1976** may attract penalty under the act.

(xii) Encashment of Interest / Dividend warrant, Refund Order, etc. :-

The Reserve Bank of India has been receiving several complaints from companies/ investors against interception of the interest/dividend warrants, refunds orders, etc. issued by various companies/institutions by unscrupulous persons who get them fraudulently encashed at branches of commercial/cooperative banks. The RBI has further opined that due to laxity on the part of officials at some banks in adhering to the guidelines / procedures for opening/operating of accounts to safeguard banks' interest, such unscrupulous persons have been successful in opening new savings/current accounts in fictitious names mainly to encash the instruments fraudulently acquired. These accounts are opened without proper introduction and in most of the cases the addresses given are fictitious.

It is reiterated that branches should scrupulously follow all the guidelines for opening/operating of accounts as provided in the manual of instructions on SB/ Current Account/Term Deposits.

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 state -ment in the form. The official incharge 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	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

receipt of any other income chargeable to Income Tax	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 to their respective controlling offices. The controlling offices are also required to appraise the Head office regarding transactions of suspicious nature.

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.

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 KYCGuidelines 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 ofRs.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.

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.

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:

	Reporting by	**Reporting to**
1.	Branch	Controlling office
2.	Controlling office	Principal Officer (P O). H.O.
3.	Principal Officer (P O). H.O.	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.

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.

(i) Risk Management :-

The inadequacy or absence of KYC standards can subject the Bank to serious customers and counter party risks especially **reputational, operational, legal and concentration risks**. **Reputational Risk** is defined as the potential that adverse publicity regarding the Bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. **Operational Risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. **Legal Risk** is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank. **Concentration Risk** although mostly applicable on the asset side of the balance sheet, may affect the liabilities side as it is also closely associated with funding risk, particularly

the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. It is worth noting that all these risks are interrelated. Any one of them can result in significant financial cost to the Bank as well as the need to divert considerable management time and energy to resolving problems that arise.

Customers frequently have multiple accounts with the **Branches**, but in offices located at different places. To effectively manage the reputational, compliance and legal risk arising from such accounts, **Branches** should be able to aggregate and monitor significant Balances and activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

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.**

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.

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 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.

Customer Education

The 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.

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.

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.

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.

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 for10 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.

Basel Committee on banking supervision requires that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Financial institutions should keep records on customer identification, account files and business correspondence for at least five years after the account is closed.

Reserve Bank of India requires that all financial transactions records should be retained for at least 5 years after the transaction has taken place and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

Branches may refer to the guidelines on 'Correspondence, Filing, Preservation, Destruction of Old Records and Reconstruction of Accounts' in respect of record keeping and be guided by the instructions therein. However, where the instructions are in contravention to the Basel norms and the RBI requirements as mentioned above, RBI instructions shall prevail.

Maintenance of records of transactions / Information to be preserved / Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit-India (FIU-IND)

Maintenance of records of transactions (nature and value)

(1) Every banking company or financial institution or intermediary, as the case may be, shall maintain a record of, -

(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 valued 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 or where any forgery of a valuable security or a document has taken place facilitating the transactions;

(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 :

(a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or

(b) travellers cheques, or

(c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or

(d) any other mode in whatsoever name it is referred to

(ii) credits or debits into or from any non-monetary accounts such as de-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-

(a) payment orders, or

(b) cashiers cheques, or

(c) demand drafts, or

(d) telegraphic or wire transfers or electronic remittances or transfers, or

(e) internet transfers, or

(f) Automated Clearing House remittances, or

(g) lock box driven transfers or remittances, or

(h) remittances for credit or loading to electronic cards, or

(i) 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:

(a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, inter Bank participation or any other investments in securities or the like in whatever form and name it is referred to, or

(b) purchase and negotiation of bills, cheques and other instruments, or

(c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or

(d) 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."

Rule 10

(1) Every banking company or financial institution or intermediary, as the case may be, shall maintain the records of the identity of its clients.

(2) The records of the identity of clients shall be maintained in hard and soft copies in a manner as may be specified by the Reserve Bank of India [or the Securities and Exchange Board of India or the Insurance Regulatory and Development Authority, as the case may be,]* from time to time.

(3) The records of the identity of clients shall be maintained for a period of ten years from the date of cessation of the transactions between the client and the banking company or financial institution or intermediary, as the case may be."

(i) Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

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 or a document has taken place facilitating the transaction and

d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

(ii) Information to be preserved

Banks are required to maintain the following information in respect of transactions referred to in Rule 3:

a) the nature of the transactions;

b) the amount of the transaction and the currency in which it was denominated;

c) the date on which the transaction was conducted; and

d) the parties to the transaction

(iii) Maintenance and Preservation of record

a) Banks are required to maintain the records containing information in respect of transactions referred to in Rule 3 above. Banks should take appropriate steps 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. Further, banks should maintain for at least ten years from the date of cessation of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

b) Banks should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.

c) Branches have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

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.

A. **Introduction of New Technologies - Credit cards/debit cards/ smart cards/gift cards**

Branches should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

Correspondent relationship with a "Shell Bank"

Banks should refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks 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.

Applicability to branches and subsidiaries outside India

The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

B. **Wire Transfer**

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

The salient features of a wire transfer transaction are as under:

- Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
- Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
- Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
- The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.
- Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, banks must ensure that all wire transfers are accompanied by the following information:

(A) Cross-border wire transfers

All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

Information accompanying cross-border wire transfers mustcontain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included. **iii)** Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

(B) Domestic wire transfers

Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

i) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

ii) When a credit or debit card is used to effect money transfer, necessary information as (i) above should be included in the message.

iii) **Exemptions**

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

Role of Ordering, Intermediary and Beneficiary banks

A. Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

B. Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

C. Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

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.

Principal Officer

The GENERAL MANAGER in charge of P&MIS Department at the Head Office 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 FIUIND.
- 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.

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.

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.

Combating Financing of Terrorism

a) In terms of PMLA Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Branches are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist

links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all Branches. Branches should ensure to update the consolidated list of individuals and entities as circulated by the Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Branches are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, Branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

c) Branches are also advised to take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions viz. Iran, Uzbekistan, Pakistan, Turkmenistan and Sao Tome and Principe, as identified in FATF Statement of February 25, 2009 circulated to banks vide our circular letter DBOD.AML. No.20716/14.01.027/2008-09 dated June 03, 2009.

Annexure – I

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 though 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 and changes in Act / Rules

- ✓ 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/	To interview the potential customer
Officer vested with the authority to open new accounts	- 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 I 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 appro-priate 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.

Prevention of Terrorism Ordinance, 2001 - Implementation thereof

Watchful eye on transactions of 23 organizations :-

In pursuance of promulgation of Prevention of Terrorism Ordinance, 2001 dated 24.10.2001, for dealing with terrorist activities and matter connected therewith, 23 terrorist organizations have been identified by the Govt. of India.

RBI, in consultation with Govt. of India has decided that branches / offices should keep a watchful eye on the transactions of these organizations.

In case of any violation of the extent Acts or normal banking operations, the matter must be reported by the concerned branch to the appropriate authorities under the Ordinance as detailed in addendum, under advice to P & D Section of Head office immediately so as to enable the Bank to report the matter to RBI.

1. It has been advised to update the consolidated list of individuals / entities as circulated by Reserve Bank as and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received. Before opening any new account, it should be ensured that the name/s of the proposed customer does not appear in the list. Further all existing accounts are to be scanned to ensure that no account is held by or linked to any of the entities or individuals included in the list. Branches have been advised that full details of accounts bearing resemblance with any of the individuals / entities in the list should immediately be intimated to RBI and FIU-IND.

2. The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. Similarly, list will be issued on individuals/entities as per Implementation of Requests Received from Foreign Countries under U.N. Security Council Resolution 1373 of 2001. Copy of the UAPA Order dated August 27, 2009 is provided in Annexure 1.

3. The designated lists will be communicated to the branches as and when received from the RBI. Provision will be made for maintaining the updated designated lists, as per UAPA.

(i) In case, the particulars of any of the customers match with the particulars of designated individuals / entities, the branches shall **immediately inform over telephone and Fax** full particulars of the funds, financial assets or economic resources or related services held in the form of bank

accounts, held by such customer on their books directly to the Joint Secretary (IS.I), Ministry of Home Affairs at Fax No.011-23092569 and also convey over Telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on **e-mail-id: jsis@nic.in** not later than 24 hours from the time of finding out such customer.

(ii) A copy of the communication mentioned in (i) above is also to be sent to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, Centre - 1, 4th Floor, Cuffe Parade, Colaba, Mumbai – 400005 and also by fax at No.022-22185792. The particulars apart from being sent by post / fax should necessarily be conveyed on **e-mail-id: cgmicdbodco@rbi.org.in.**

(iii) A copy of the communication mentioned in (i) above is also to be sent to the UAPA nodal officer of the state / UT where the account is held as the case may be and to FIU-India.

(iv) A copy of the above is also to be sent to the concerned Regional office and to the Principal officer, Development Wing, H.O. not later than 24 hours from the time of finding out such customer.

(v) In case, the match of any of the customers with the particulars of designated individuals / entities is beyond doubt, the Principal Officer should direct branches to prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011- 23092736.

(vi) Branches shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (i) above, carried through or attempted, as per the prescribed format.

4. Freezing of Financial Assets

i) On receipt of the particulars as mentioned in paragraph 4 (i) above, IS-I Division of MHA would cause a verification which would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

ii) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals / entities, an order to freeze these assets under section 51A of the UAPA would be issued by The Joint Secretary (IS-I), MHA within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.

The order shall take place without prior notice to the designated individuals / entities. Branches shall provide a copy of the order to Principal Officer, Development Wing, H.O. through the concerned Regional office.

5. Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals / entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person.

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned / held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned branch. The

branch shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4(i) of this Circular within two working days with a copy to The Principal Officer, Development Wing, H. O. and concerned Regional Office. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual / entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned / held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.