

**THE KRISHNA DISTRICT CO.OPERATIVE CENTRAL BANK LTD.,
MACHILIPATNAM**

**KYC POLICY
POLICY GUIDELINES ON KYC/AML/CFT-2013-14**

1. Objective

i. Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT)

- a) The objective of KYC / AML / CFT guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.
- b) KYC procedures also enable Bank to know / understand the customers and their financial dealings better which in turn help to manage the risks prudently.
- c) The Board approved policy on KYC / AML / CFT is subject to annual review.

2. Definition of Customer

- i. For the purpose of KYC policy, a 'Customer' is defined as:
 - a) A person or entity that maintains an account and / or has a business relationship with the bank;
 - b) One on whose behalf the account is maintained (i.e. the beneficial owner);
 - c) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
 - d) Any person 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.
 - e)** Rule 9(1A) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

- f) A juridical person has been defined as an Entity, as a firm, that is not a single natural person, as a human being, authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).
- ii. The RBI and the Government of India have now advised the procedure for determination of Beneficial Ownership as under:

a) Where the client is a person other than an individual or trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

- I. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company; ownership of/entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or, ownership of/entitlement to more than 15% of the property or capital or profits of the juridical person where the juridical person is an unincorporated association or body of individuals.

- II. In cases where there exists doubt under (i) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements, etc

- III. Where no natural person is identified under (I) or (II) above, the identity of the relevant natural person who holds the position of senior managing official.

b) Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

3. Guidelines

i. General

- a) Bank shall keep in view 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. Bank shall, therefore, ensure that 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 shall be sought separately with his / her consent and after opening the account.
- b) Bank shall ensure that any remittance of funds by way of demand draft, mail / telegraphic transfer or any other mode and issue of travelers' cheques /sale of gold coins, etc. for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.
- c) Bank shall not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.
- d) Bank shall ensure that the provisions of Foreign Contribution (Regulation) Act, 1976, as amended from time to time, wherever applicable are strictly adhered to.

4. Banking Department

- i. The Banking Department of the Krishna DCCbank will attend to functions with regard to KYC/AML/CFT matters are as follows:
 - a) Issuance of guidelines pertaining to KYC/AML/CFT for deposits and implementation/monitoring of the same.
 - b) Verification of implementation of KYC/AML/CFT guidelines including liaison with RBI/IBA/FIU/other agencies, reporting to regulatory authorities and AFI team of RBI apart from attending to STR,CTR and CCR alerts.

5. Key Elements of KYC Policy

- i. The KYC Policy includes the following four key elements:
 - a) Customer Acceptance Policy;
 - b) Customer Identification Procedures;
 - c) Monitoring of Transactions; and
 - d) Risk Management.

6. Customer Acceptance Policy (CAP)

- i. Bank shall ensure the following aspects of customer relationship in the bank.
 - a) No account is opened or maintained in anonymous or fictitious / benami name(s);
 - b) Necessary checks are done before opening a new account so as to ensure 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 etc.
 - c) Bank shall 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 bank shall 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 will not be divulged for cross selling or any other purposes.
 - d) 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 shall be verified.

7. Risk Perception in respect of Customer

- i. "Customer risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's

perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by Customer.

ii. 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.

iii. **Low Risk Customers (Level 1 customers)**

a) 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 confirm to the known profile may be categorized as Low risk.

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

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

iv. **Medium Risk Customers (Level 2 customers)**

a) Customers who are likely to pose a higher than average risk to the bank should be categorized as medium or high risk.

b) 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 identification.

c) The following customers are classified as **Medium Risk Customers:**

- Gas Dealers
- Car/boat/plane dealers
- Electronics
- Travel agency
- Telemarketers
- Telecommunication service providers
- Pawnshops
- Auctioneers
- Restaurants, Retail shops, Movie theatres, etc.
- Sole practitioners

- Notaries
- Accountants
- Blind
- Purdanashin
- Registered body

v. **High Risk Customers (Level 3 customers)**

a) 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 identification. **Bank shall subject such accounts to enhanced monitoring on an ongoing basis.**

- 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).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers, etc.
- High Net worth Individuals*
- Non-Resident Accounts.
- Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewelers.

Parameters for defining High Net worth Individuals:

Customers with any of the following:

- Average balance of Rs. 2.00 lakh and above in SB/NRE SB.
- Balance of Rs. 10.00 lakh and above in Term deposit, Domestic/NR.
- Balance of Rs.5.00 lakh and above in CA.
- Enjoying Fund based limits/term loans exceeding Rs. 30.00 lakh.
- Salary credit of **Rs. 1,00,000/-** and above in a saving salary A/c.
- Business contribution/opinion makers /VIPs such as head of village/Town/City, Top Executives of Companies etc.

vi. 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.

- vii. Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, branches should carry out full scale customer due diligence (CDD) before opening an account.
- viii. Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of business relationship.
- ix. Bank shall have a system of periodical Updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such Updation shall not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.
- x. Bank will not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and / or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data / information furnished to the bank.
- xi. The bank shall take steps to identify and assess the ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels. Bank shall have controls and procedures in place to effectively manage and mitigate the risk adopting a risk-based approach. As a corollary, bank would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating.
- xii. RBI has directed that Banks are required to prepare a Risk profile of each customer and apply enhanced due diligence measures on High risk customers. IBA has provided an indicative list of High/Medium risk Products, Services, Geographies, locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure II).

8. Customer Risk Categorisation

- a) Banks may choose to carry out either manual classification or automatic classification or a combination of both. Similarly for selecting parameters, Bank may select the parameters based on the available data. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter.

b) Bank shall adopt combination of manual and automatic classification. Based on the availability of data, Bank shall finalise parameters which are available in the system and the same shall be reviewed annually. System shall assign provisional risk categorization based on the system provided parameters. Branches shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy.

c) Bank shall prepare a profile for all Customers 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 client's business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. Risk categorization shall be done based on selection of parameters and assigning suitable risk category.

d) **Risk Parameters**

a) The first step in process of risk categorization is selection of parameters, which would determine customer risk.

b) Banks on KYC/AML/CFT/Obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used to determine the profile and risk category of Customers:

1. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
2. Business Segment : Retail, Corporate etc
3. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national.
4. Product Subscription: Salary account, NRI products etc.
5. Economic Profile: HNI, Public Ltd. Company etc.
6. Account Status: Active, inoperative, dormant.
7. Account Vintage: Less than six months old etc.
8. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.
9. Suspicious Transaction Report (STR) filed for the customer.
- 10.AML alerts

c) Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc can also be used in addition of the above parameters. Bank shall adopt all or majority of these parameters based on availability of data.

e) **Risk rating of Customers:**

a) Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of

origin, sources of funds and client profile etc.

b) An Illustrative list of Low/Medium/High Risk Customers, Products, Services, Geographies etc., based on the recommendations of IBA Working Group on Risk Based Transaction Monitoring is detailed in Annexure II.

c) Risk rating based on the Deposits/account balance:

Account Types	High	Medium	Low
Only SB*	Rs. 2,00,000/- & above	Rs. 1,00,000/- & above but less than Rs.2,00,000/-	Less than Rs.1,00,000/-
Only Current*	Rs. 5,00,000/- & above	Rs. 2,00,000/- & above but less than Rs.5,00,000/-	Less than Rs.2,00,000/-
Only Deposits Term	Rs. 10,00,000/- & above	Rs. 5,00,000/- & above but less than	Less than Rs.5,00,000/-

*Applicable in case of accounts having completed 6 months

f) For Current/SB accounts average balance for last 6 months and for Term Deposits principal amount shall be taken for consideration on the date of review.

g) If a customer is having more than one of the above categories of accounts, highest risk assigned for the above parameter shall be the overall risk for this parameter. For ex: A customer having a savings account with average balance of Rs.1,50,000/-(medium) and Term Deposit of Rs.4,00,000/-(low) shall have rating of Medium Risk for this parameter.

h) Above categorization of the Customer shall be based on all accounts linked to CUST ID irrespective of constitution of account like Joint account, Partnership account etc. However accounts linked to CUST ID where customers do not have any stake in Business/activity need not be clubbed for the above purpose.

i) Risk Categorisation of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

1. Unusual transaction/behavior (given as Annexure III – Monitoring of Customer Risk Categorisation (CRC).
2. Submitted Suspicious Transaction Reports (STR) for Customer.

3. Submitted Cash Transaction Report (CTR).
4. Frequent cheque returns.
5. Minor.

j) Risk Categorisation of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer. For ex: a Travel Agent (Medium risk) with Proprietorship account (low risk) and having Savings account with average balance of Rs.1,50,000/- (medium risk) and Term Deposit of Rs.4,00,000/- (low risk) , shall be assigned with overall rating of "Medium Risk", provided all other conditions mentioned under C above does not necessitate for assigning "High Risk".

k) **Risk categorization of Customers undertaken by the Bank:**

Based on the policy/guidance notes of RBI/IBA and also the methodology of Customer Risk Categorisation provided (as detailed under points A, B & C above), risk rating has been assigned taking into account the following parameters available in CBS system :

- Customer type.
- Customer Profession.
- Type of business.
- Product code.
- Account status
- Account vintage.

- Average balance/deposits in SB/Current/Term Deposit accounts.

9. THE ROLES AND RESPONSIBILITIES OF AUTHORITIES FOR CUSTOMER RISK CATEGORISATION (CRC):

i. **Roles and responsibilities of Branches:**

- Branches shall review Customer risk categorization based on the risk categorization generated by the system, every six months, as on 15th of May and November every year.
- Branches may also apply additional alert indicators to address specific risks faced by them.

ii. **Roles and responsibilities of Nodal officers:**

- Shall monitor/follow-up process of review/classification/re-classification of Customer risk categorisation.

- Shall ensure compliance of Risk categorization at branches every six months.
- Shall submit periodical reports on implementation/review of risk categorisation to Banking Dept, H.O.
- Shall attend/follow-up audit observations/remarks.

iii. **Banking Department, H.O:**

- Oversee implementation/monitoring and review of risk categorization of customers by putting in place suitable reporting/monitoring mechanism.
- Ensure proper maintenance of MIS for customer risk categorization and migration data.
- Shall review fixing of parameters available through the system annually.

iv. **Inspection Wing, H.O:**

- Shall review and provide necessary recommendations/directions to strengthen adherence of KYC/AML guidelines.
- Shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

10)Monitoring/Review of Customer Risk Categorisation (CRC):

- i. Branches shall carry out a review of risk categorization of customers at a periodicity of not less than once in six months i.e., as on 15th of May and November every year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.
- ii. Wherever there is suspicion at branch level that a Customer is above low risk, branches should carry out customer due diligence (CDD) before opening an account.
- iii. Based on objective parameters for enhanced due diligence, branches shall arrive at a conclusion whether the transaction is suspicious or not. Some of the objective parameters could be for enhanced due diligence could be:
 - A. Customer locations.
 - B. Financial Status
 - C. Nature of business.
 - D. Purpose of transaction.

- iv. The IBA Working Group had recommended 88 alert indicators for detection of suspicious transactions for implementation by all the Banks. AML package version 4.2 has been released for submission of alert reports as per the recommendations of "IBA Working Group". However, out of the above 88 alert indicators, 27 alert indicators pertain to off-line transactions and Branches shall submit the 27 offline alert reports in the AML package itself. The list of 27 offline alert indicators is provided in Annexure III.

Monitoring of Customer Risk Categorization (CRC) – given as Annexure III.

11. Customer Identification Procedure

- i. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Bank shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer and the purpose of the intended nature of banking relationship. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).
- ii. The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within the bank. To achieve this, the bank shall issue Unique Customer Identification Code (UCIC) for each customer. The UCIC will help the bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the bank to have a better approach to risk profiling of customers.
- iii. Branches are required to strictly avoid creating multiple customer IDs while opening new accounts and in case of existing multiple IDs, branches have to complete the process of de-duplication.
- iv. Opening of a new account should be authorised only by the Manager/ Senior Manager in charge of the branch/ Department. In larger branches, however, Officer-in-Charge of the Department shall authorise opening of new account subject to fulfillment of other conditions. Branches to ensure that the features and restrictions in the deposit products are to be explained to the customers and the appropriate product code is selected at the time of opening an account basing on the needs and choice of the customers.
- v. **Introduction of accounts:**
 - a) Introduction from an existing customer is not mandatory for opening accounts,

including those of legal entities. After passing of PML Act and introduction of document based verification of identity/address of the proposed account holders, the accounts opened with proper documents are considered as acting in good faith and without negligence by the banks.

- b) If an existing account holder intends to open another account with a different branch, fresh account opening form/letters duly completed by the account holder, should be attested/ introduced by the branch, only if the present account of the person/firm has been operated satisfactorily for a period of one year during the immediately preceding year. These forms are to be sent directly by Registered Post A.D. to the branch where the existing account holder wants to open a fresh account. When an account opening form in which a person/s or a firm is duly introduced by one of our branches is received by Regd. Post, the account opening branch should immediately seek confirmation of introduction in such account opening form from the account introducing branch by addressing a letter. The account opening branch should exercise caution on operations in such newly opened accounts till confirmation is received from the introducing branch. The account opening branch shall necessarily obtain independent confirmation of address of the person/firm as is being done in case of new account.

vi. Customer identification documents:

- a) An indicative list of the nature and type of documents/ information that may be relied upon for customer identification is given in Annexure I. Permanent correct address, as referred in Annexure I means the address at which the person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the Bank. Branches may also accept Job card issued by NREGA duly signed by an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number as officially valid KYC documents for the purpose of opening of accounts.
- b) If the address provided by the prospective customer in the account opening form is the same as that on the document submitted for identity proof, the document may be accepted as a valid proof of both identity and address. If however, the address indicated in the documents submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address should be obtained. For this purpose, apart from the indicative list of documents detailed in Annexure-I, a rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

c) Acceptance of Aadhaar letter for KYC compliance:

If the address provided by the account holder is the same as mentioned in the Aadhaar letter, it may be accepted as a proof of both identity and address. If however, the address indicated in the documents submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address should be obtained.

d) Acceptance of NREGA Job Card for KYC compliance:

NREGA Job Card duly signed by an officer of the State Government can be accepted as an officially valid document for opening of bank accounts without the limitations applicable to "Small Accounts".

e) Customer data enrichment in CBS should be a continuous process. Customer information like PAN No., Aadhaar No. Passport No., Driving Licence No., Mobile Telephone No., income details, business type, profession/occupation type, etc. should be updated in the CBS.

vii. Thanks Giving letter

a) In respect of all newly opened accounts, a Thanks Giving letter shall be sent to the new account holder. This would while earning the goodwill of the customer also serves as a confirmation of address.

b) If the Thanks Giving letter so sent is returned undelivered, the branch should immediately take appropriate action to safeguard the interest of the bank.

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

viii. Precautions to be exercised in case of joint accounts

a) The mode of operation should be noted in red ink on the top of specimen signature card. This note in the specimen signature card should be checked and initialed by the Branch Official.

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

c) All prospective joint account holders are to be KYC compliant.

d) Transfer of accounts from one branch to another branch cannot be done at the request of any one of the joint account holders.

ix. Opening of Current Account with non-consortium banks

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

x. Accounts under Foreign Contribution Regulation Act, 1976 (FCRA)

- a) In terms of the Foreign Contribution Regulation Act, 1976, certain categories of individuals and organizations are required to obtain prior permission from the Central Government (Secretary, Ministry of Home Affairs, GOI, New Delhi) to receive "Foreign Contributions" or accept "Foreign Hospitality" and such receipts/acceptance require reporting to the Government.

I. Individuals/Organizations who cannot receive foreign contributions :
Foreign contributions cannot be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employee of any corporation, member of any legislature, political party or office bearer thereof.

II. 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.

xi. Need for photographs and address confirmation:

- b) Pass port size/stamp size photograph of the depositors should be obtained in case of all Current Accounts, SB accounts and Term Deposits.
- c) In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public/private limited companies, HUF, trusts, Limited Liability Partnerships etc., and those of minors, photographs of the authorised signatories should be obtained. Photographs of the student account holders should be attested by the school authorities on the reverse.
- d) In case of change in the authorised signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organisations.
- e) Photograph should be obtained in case of NRI accounts also.

- f) Where the accounts are operated by letters of authority, photographs of the authority holders should be obtained, duly attested by the depositors.
- g) In cases where some close relatives e.g. wife, son daughter and parents etc. who live with their husband, father/ mother and son finding difficulty in opening accounts 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.

xii. Shifting of bank accounts:

- a) KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC had been done for the concerned account. The customer should be allowed to transfer his account from one branch to another branch without restrictions. In order to comply with KYC requirements of correct address of the person, fresh address proof has to be obtained from him/her upon such transfer by the transferee branch.
- b) A large number of customers with transferable jobs or those who migrate for jobs are unable to produce a utility bill or other documents in their name as address proof immediately after relocating. With a view to further easing the KYC process for the general public, especially customers who migrate to a new place on account of new job, transfer, etc., the existing guidelines on transfer of bank accounts from one centre to another are modified as under:
 - A. Branches may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address, subject to submitting proof of address within a period of six months.
 - B. Branches may also accept rent agreement duly registered with State Government or similar registration authority indicating the address of the customer, in addition to other documents listed as proof of address in Annexure-I.
- c) Branches shall display a notice prominently in their Banking Hall to intimate the customers that in the event of change in address due to relocation or any other reason, they should intimate the new address to the bank within two weeks of such a change. While opening new accounts and while periodically updating KYC data as required in terms of the KYC/AML/CFT guidelines, an undertaking to this

effect should be obtained. In all these cases customers will have to produce proof of address as mentioned at (A) and (B) above.

9. Customer Identification Requirements - Indicative Guidelines

i. Walk-in Customers

- a) 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. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/- the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND.
- b) The identity and address of the Walk-in customer is to be verified by obtaining KYC documents and records are to be maintained/ updated in the system. Bank shall also verify the identity of the customers for all international money transfer operations.

ii. Salaried Employees

- a) In case of opening of bank account of salaried employees of Corporates and other entities, Branches should accept letter / certificates issued by the employer as a KYC document, only in case it is issued by the competent authority of Corporates/ reputed entities

.In addition to the certificate/ letter from the employer, Branches should also invariably obtain at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules or utility bills for opening bank account of salaried employees of Corporates and other entities.

iii. Trust / Nominee or Fiduciary Accounts

- a) There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Bank shall determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, Bank shall 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.
- b) While opening an account for a trust, Bank shall 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 shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

iv. Accounts of companies and firms

- a) Bank need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Bank shall 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.

v. Client accounts opened by professional intermediaries

- a) When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client shall be identified. Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Bank also maintains 'pooled' accounts managed by lawyers / chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners shall be identified. Where such funds are co-mingled at the Bank, the Bank shall still look through to the beneficial owners. Where the Bank rely on the 'customer due diligence' (CDD) done by an intermediary, Bank will see that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.
- b) Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that Bank will not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc. who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits Bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, shall not be allowed to open an account on behalf of a client.

vi. Accounts of Politically Exposed Persons (PEPs) resident outside India

- a) 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. Bank shall 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. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. Branches should maintain a database of PEP accounts in the Branch. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.
- b) The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming a Politically Exposed Person (PEP), has to be taken by branch head in branches headed by Branch Manager and above.
- c) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where a PEP is the ultimate beneficial owner shall be categorised 'high risk' so that appropriate transaction alerts are generated and the accounts are subjected to enhanced CDD on an ongoing basis.

vii. Accounts of non-face-to-face customers

- a) 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 shall be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents may be called for. In such cases, Bank may also require the first payment to be effected through the customer's account with another bank which, in turn, follows KYC procedures. 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. In

such cases, it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

viii. Accounts of Proprietary Concerns

- a) Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, Bank shall call for and verify the following documents before opening of accounts in the name of a proprietary concern:
- b) Proof of the name, address and activity of the concern, like Registration Certificate (in the case of a Registered concern), Certificate/Licence issued by the Municipal Authorities under Shop and Establishment Act, Sales and Income Tax Returns, CST/VAT Certificate, Certificate/Registration document issued by Sales Tax/ Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, Registration /licensing document issued by Central Government or State Government Authority/ Department, IEC (Importer Exporter Code) issued by the office of DGFT, etc.
- c) Complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities.
- d) Utility bills such as Electricity, Water and landline Telephone bills in the name of the proprietary concern.
- e) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.
- f) These guidelines on proprietorship concerns will apply to all existing and new customers.

ix. Accounts of Non Profit Organisations

- a) Non Profit Organisation (NPO) means any entity or organisation that is registered as a Trust or a Society under the Societies Registration Act, 1860 or any similar State Legislation or a company registered under Section 25 of the Companies Act 1956. All transactions involving receipts by these NPOs of value more than Rs.10 lac or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 lac, the Bank shall consider filing a

x. Accounts of migratory workers

- a) Branches may open accounts of migratory workers based on the proof of permanent address also. This account may be opened under small value accounts by adopting simplified KYC procedure.

xi. Accounts of SHGs:

- a) In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening Savings Bank accounts and credit linking of their accounts, the Reserve Bank of India has decided to simplify certain norms for SHGs. Accordingly, KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.
- b) As regards KYC verification at the time of credit linking of SHGs, it is clarified that since KYC would have already been 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.

xii. Accounts operated by Power of Attorney Holders/Letter of Authority Holders:

- a) In case of accounts operated by Power of Attorney (POA) Holders / Letter of Authority (LOA) Holders, KYC documents are to be obtained from such POA holders/ LOA holders and records are to be maintained/ updated in the system.

xiii. Beneficial Owners:

- a) Branches shall obtain details of Beneficial Owners, wherever applicable and maintain records/ update in the system.

xiv. Basic Savings Bank Deposit Accounts

- a) The "Basic Savings Bank Deposit Account" shall offer following minimum common facilities to all the customers:
 - I. The Basic Savings Bank Deposit Account shall be considered a normal banking service available to all.
 - II. This account shall not have the requirement of any minimum balance.

- III. The services available in the account will include deposit and withdrawal of cash at bank branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.
 - IV. While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a maximum of four withdrawals in a month, including ATM withdrawals; and
 - V. Facility of ATM card or ATM-cum-Debit Card.
- b) The above facilities will be provided without any charges. Further, no charge will be levied for non-operation/ activation of inoperative Basic Savings Bank Deposit Account.
 - c) Additional value added services beyond the stipulated basic minimum services will be chargeable.
 - d) The Basic Savings Bank deposit Account would be subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time. If such account is opened on the basis of simplified KYC norms, the account would additionally be treated as a "Small Account" and would be subject to conditions stipulated for such accounts are detailed under Accounts with Relaxed KYC guidelines.
 - e) Holders of Basic Savings Bank Deposit Account will not be eligible for opening any other savings bank deposit account in the bank. If a customer has any other existing savings bank deposit account in the bank, he/she will be required to close it.

xv. Accounts with Relaxed KYC Guidelines – "SMALL ACCOUNTS"

- a) Although flexibility in the requirements of documents of identity and proof of address has been provided in the KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annexure I, Bank shall open an account with Relaxed KYC guidelines.
- b) The accounts with "Relaxed KYC guidelines" can be opened . The features of the above account and restrictions stipulated by RBI/Govt. of India are as follows:

- accounts where aggregate of all credits in a financial year does not exceed Rs.1.00 lac;
 - the aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000/- and
 - where the balance at any point of time does not exceed Rs.50,000/-.
- c)** Any violation of the stipulations mentioned above will result in restraining the operations in the account after giving due notice to the account holder.
- d)** Small Savings Bank Deposit account can be opened on production of a self attested photograph and affixation of signature or thumb impression as the case may be, on the form for opening the account, provided that the bank official while opening the account certifies under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence.
- e)** This account can also be opened by submitting the NREGA job card duly signed by an officer of the State Government, or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, etc.
- f)** A Small Savings Bank Deposit Account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the Bank of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.
- g)** A Small Savings Bank Deposit Account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of customer shall be established through the production of officially valid documents.
- h)** Foreign remittances shall not be allowed to be credited into a Small Savings Bank Deposit Account unless the identity of the customer is fully established through the production of officially valid documents.

xvi. Money mules

- a) Money mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering.

Money mules receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or other individuals, minus a certain commission. Branches should strictly follow the KYC /AML/CFT guidelines to prevent abuse of banking system by money launderers using money mules.

xvii. Bank no longer knows the true identity

- i. In the Circumstances when the Bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the Bank shall also file an STR with FIU-IND.

12. Monitoring of Transactions

- ii. Ongoing monitoring is an essential element of effective KYC procedures. Bank can effectively control and reduce the risk only if Bank has an understanding of the normal and reasonable activity of the customer so that Bank has 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. Bank shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Bank has prescribed threshold limits for a particular category of accounts and particular attention is paid to the transactions which exceed these limits. Attention is also paid to transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. 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 are subjected to intensified monitoring. High risk associated with accounts of bullion dealers (including sub-dealers) and Jewelers are to be taken in to account to identify suspicious transactions for filing suspicious transaction reports (STRs) to FIU-IND. Bank has 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 is to be carried out at a periodicity of not less than once in six months.
- iii. Bank shall closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheques are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates, the bank shall carefully analyse such data and in case any unusual operations are found in the accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-Ind.

- iv. Bank shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.
- v. Branch Managers should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt necessary enquiries be made with the account holders.
- vi. While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.
- vii. Branches are advised to mandatorily obtain either PAN or Form 60/61 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for ` 50,000/- and above. If the customer appears to be structuring the transactions into a series of transactions below the threshold of ` 50,000/-, branches are required to obtain PAN or Form 60/61.
- viii. If PAN is not available) from the customer. Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of abstention of PAN or Form 60/61, wherever the aggregate amount of transactions is ` 50,000/- and above. Branches are advised to collect appropriate charges for the aggregated transactions.
- ix. All the staff members are instructed to maintain the standards of good conduct and behavior expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.
- x. Fictitious offers of cheap funds from abroad- adherence to KYC/AML Guidelines in opening/monitoring of transactions in accounts:
 - a) It has been reported that there has been an increase in instances of fictitious offers, where fraudsters are using RBI's corporate logo/name in their email messages, and also sometimes including the photograph of the Governor to convince the victims of the authenticity of the purported messages conveying lottery/prize winnings. The fraudsters persuade victims into making initial payment into a specific bank account towards charges for claiming the prize money. The victims complain to RBI after they have lost money in such transactions. It is observed from the responses received from banks in this regard that these transactions generally take place in newly opened accounts of

individuals/ salary accounts, which are classified as low risk.

- b) RBI has issued various advisories on its website, warning public against falling prey to fictitious offers/ lottery winnings/ remittance of cheap funds in foreign currency from abroad by so-called foreign entities/ individuals or to Indian residents acting as representatives of such entities/ individuals.
- c) In view of the above the following guidelines are reiterated:
 - a. Branches should ensure strict adherence to the KYC/AML guidelines issued from time to time relating to opening of accounts, risk categorization of accounts and monitoring of transactions in accounts.
 - b. Generally the fraudsters open and route transactions through salary/ savings accounts. The transactions that are deviating from the threshold limit/ outside the normal transaction region should be probed into.
 - c. Branches should closely monitor newly opened accounts in the initial 6 months and due diligence to be applied to transactions not in line with the customer profile.
 - d. Staff members in the Front office/ operations desks should be sensitized to handle queries from customers regarding such lottery winnings where the customers have been advised to deposit money in specified accounts.

xi. **Closure of accounts**

- a) Where the branch is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken by the Branch-in-charge.
- b) While it is absolutely necessary for banks as well as customers to comply with the measures prescribed for KYC/AML purposes, drastic measures like closing of accounts may be taken only after sending out sufficient discernible warning signals to the customers having regard to the level of customer education and public awareness on the subject. In all such cases where the account holders are either not responding over a period of time/not found at the given address, bank may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

c) Before taking the extreme step of closing an account on account of noncompliance with the KYC/AML requirements, as an initial measure, branches are advised to place such accounts under close watch, depriving the non-compliant customers certain additional facilities, till the customer complies with such requirements. This exercise, however, should not extend beyond a period of three months. If the customer despite such measures, shows unwillingness to comply with KYC/AML/ CFT requirements, branches would be free to proceed further and close the accounts after giving due notice to him/her. It is reiterated that basic banking transactions already in force should not be disturbed for meeting KYC review requirements.

13. Risk_Management

- i. The inadequacy or absence of KYC standards can subject the Bank to serious customer 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 assets 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.
- ii. Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, compliance and legal risk arising from such accounts, Bank shall 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.
- iii. Concurrent / Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals.
- iv. **Introduction of New Technologies - Credit cards / debit cards / smart cards / gift cards**

- a) Bank shall pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Further, where marketing of these cards is done through the services of agent, Bank shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. The agents will also to be subjected to KYC measures.

v. 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. Bank has therefore developed a suitable mechanism 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 banks and financial institutions. Bank ensures to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals / entities can be accessed in the website at [http:// www.un.org/ sc/ committees/ 1267/ aq_sanctions_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml) (Al-QaidaSanctions List) and <http://www.un.org/sc/committees/1988/list.shtml> (1988 Sanctions List).. 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 shall immediately be intimated to RBI and FIU-IND.
- c) 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, also in electronic form. In case, the particulars of any of their customers match with the particulars of designated individuals / entities, the branches shall immediately inform 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. Copies of the communication mentioned shall also to be sent to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking

- d) In case, the match of any of the customers with the particulars of designated individuals / entities is beyond doubt, the Principal Officer shall direct branches to prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS-I), Ministry of Home Affairs. Branches shall also file a Suspicious Transaction Report (STR) with FIU-IND, through the Principal Officer, covering all transactions in the accounts, carried through or attempted, as per the prescribed format.

vi. Freezing of Financial Assets

- a) On receipt of the particulars IS-I Division of Ministry of Home Affairs (MHA) would cause a verification to be conducted by the State Police and / or the Central Agencies so as to ensure that the individuals / entities identified by the banks are the ones listed as designated individuals / entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals / entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars. 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 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, Inspection Wing, H.O. through MIPD Section of the concerned Circle.

- vii.** 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.

- a) 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 within two working days with a copy to the Principal Officer, H.O
- b) 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.

viii. Communication of Orders under the Section 51A of Unlawful Activities (Prevention) Act

- a) All Orders under Section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, will be communicated to the branches on receipt of communication from RBI.

ix. Domestic wire transfers

- a) 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.
- b) If a bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank shall insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.
- c) When a credit or debit card is used to effect money transfer, necessary information as (a) above should be included in the message.

x. Exemptions

- a) Inter-bank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

xi. 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. As Ordering Bank, the Bank shall ensure that qualifying wire transfers contain complete originator information. The Bank shall 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, Bank processing an intermediary element of a chain of wire transfers shall 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 shall be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) as 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. As Beneficiary Bank, the Bank shall 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 Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

xii. Principal Officer

- a) Bank has appointed a Principal Officer. Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.
- b) The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.
- c) The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to FIU-IND.

xiii. Designated Director on the Board of the Bank:

- a) Bank has nominated an Executive Director overseeing Inspection Wing of the Bank as a Designated Director on the Board of the Bank to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012. The Designated Director will oversee the compliance position of AML norms in the Bank.

xiv. 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)

- i. Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies with regard to preservation and reporting of customer account information. Bank shall take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act *ibid*.

xv. Maintenance of records of transactions

- i. Bank shall have a system of maintaining proper record of transactions 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 exceed Rupees Ten Lakh;
 - c. All transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency;
 - d. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and
 - e. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

xvi. Information to be preserved

- i. Bank shall maintain all necessary information in respect of transactions referred to in Rule 3 of PML Rules, 2005 to permit reconstruction of individual transactions, including the following information:
 - 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.

xvii. Maintenance and Preservation of records

- i. Bank shall maintain the records containing information in respect of transactions as referred above. Bank shall 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, Bank shall maintain for at least ten years from the date 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.
- ii. Bank shall 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 shall be made available to the competent authorities upon request.
- iii. Bank shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background, including all documents / office records / memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings, at branch as well as Principal Officer level, shall be properly recorded. Such records and related documents shall 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 will be preserved for ten years as is required under PMLA, 2002.

- iv. Branches may also refer to the RBI instructions on preservations of Records in banks in respect of record keeping and be guided by the instructions therein.

xviii. Reporting to Financial Intelligence Unit-India

- i. In terms of the PMLA rules, Bank is required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than Rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

The Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor,
Hotel Samrat, Chanakyapuri, New Delhi-110021.

Website - <http://fiuindia.gov.in/>

- ii. There are altogether eight reporting formats i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR.
- iii. A Report of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency shall be forwarded to FIU-IND every month by the 15th of the succeeding month.

xix. Cash and Suspicious Transaction Reports:

i. Cash Transaction Reports (CTR)

The bank shall scrupulously adhere to the following:

- a) The Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to Head Office shall, therefore, invariably be submitted on monthly basis and Bank shall ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
- b) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately, within 7 days of detection of counterfeit currency, in the specified format (Counterfeit Currency Report - CCR). These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

- c) While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.
- d) CTR shall contain only the transactions carried out by the Bank on behalf of their clients / customers excluding transactions between the internal accounts of the bank.
- e) A summary of cash transaction report for the bank as a whole shall be compiled by the Principal Officer of the bank in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted.

ii. Suspicious Transaction Reports (STR)

- a) It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. Bank shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.
- b) Bank shall make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and / or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
- c) The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.
- d) Bank shall not put any restrictions on operations in the accounts where an STR has been made. Bank and their employees shall keep the fact of furnishing of STR strictly confidential, as required under PML rules. Moreover, it shall be ensured that there is no tipping off to the customer at any level.
- e) 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, if a branch 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 branch shall verify identity and address

of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

11. Customer Education / Employee's Training / Employee's Hiring

i. Customer Education

Implementation of KYC procedures requires Bank to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, Bank may prepare specific literature / pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with customers.

ii. Employees' Training

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

iii. Hiring of Employees

KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank shall put in place adequate screening mechanism put in as an integral part of its recruitment / hiring process of personnel.

The policy may alter/modify/delete the contents from time to time. For updated information please approach nearest branch.

KYC DOCUMENTS

ANNEXURE - I

Considering the risk perspective of customer type and product risk, the following documentation has been made mandatory for accepting the customer, while opening an account.

Features to be verified and documents that may be obtained from the customers.	
Features	Documents
Accounts of individuals -- Legal name or any other names used. --Correct permanent address	Photograph and any one of the following documents. <ul style="list-style-type: none">i. Passportii. Pan Cardiii. Voter's Identity Cardiv. Driving Licence.v. Job Card issued by NREGA duly signed by an officer of the State Governmentvi. Letter issued by UIDAI containing details of name, address and aadhar numbervii. Photo Identity Card (subject to bank's satisfaction)viii. Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the bank.<ul style="list-style-type: none">i. Telephone Billii. Electricity Billiii. Bank account statementiv. Letter from any recognized public authorityv. Ration Cardvi. Letter from employer (subject to satisfaction of the bank)vii. Any document which provides customer address information to the satisfaction of the bank will suffice.<ul style="list-style-type: none">a. If the address on 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 of 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.
<p>Accounts of companies.</p> <p>-- name of the company. -- principal place of business. -- Mailing address of the company -- Telephone /Fax number</p>	<ol style="list-style-type: none"> i. Certificate of incorporation, Certificate of commencement of business and Memorandum & Articles of Association (up-to-date) certified by the Secretary/Director of the Company. ii. Resolution of the Board of Directors to open an account and identification of those who have the 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 Telephone Bill. vi. List of present Directors signed by the Chairman of the Company. vii. List of Authorised signatories with their signatures attested by the Chairman of the Company. viii. As a proof of current address at least one of the address proof of each Director and photograph of the Directors.
<p>Accounts of Partnership firms.</p> <p>--- Legal name --- Address --- Names of all partners and their addresses --- Telephone numbers of the firm and partners.</p>	<ol style="list-style-type: none"> i. Registration certificate, if registered, with a copy certified by the partners. 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. vi. Partnership letter in Bank's format.
<p>Accounts of Trusts & foundations.</p> <p>-- Names of trustees, settlors, beneficiaries and signatories. -- Names and addresses of the founder, the managers/directors and the beneficiaries. -- Telephone/fax numbers.</p>	<ol style="list-style-type: none"> 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, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses. iv. Resolution of the Managing body of the

	<p>foundation/ association for opening and operating the account signed by all the trustees.</p> <p>v. Telephone Bill.</p> <p>vi. The trust Deed for verification with copy certified by the Chairman. (The deed should empower the trustees to open Bank Account)</p> <p>vii. A list of the names of trustees with their signatures attested by the Chairman.</p>
<p>Accounts of proprietorship concern.</p> <p>-- Proof of the name, address and activity of the concern.</p>	<p>i. Proprietorship letter in Bank's format, besides identity proof & address proof.</p> <p>ii. Power of Attorney if granted by the proprietor.</p> <p>Any two of the following documents:</p> <p>iii. Registration certificate in case of a registered concern)</p> <p>iv. Certificate/Licence issued by the Municipal Authorities under Shop & Establishment Act.</p> <p>v. Sales & Income Tax Return</p> <p>vi. CST/VAT certificate</p> <p>vii. Certificate/ registration document issued by Sale Tax/Service Tax/Professional Tax Authority.</p> <p>viii. License issued by the Registering authority like Certificate of Practice issued by the Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food & Drug Control Authorities</p> <p>ix. Any registration/ licencing document issued by the Central Govt. or State Govt. authority/Department.</p> <p>x. Importer Exporter Code issued to the proprietorship concern by the Office of the Directorate General of Foreign Trade.</p>
<p>Accounts of Salaried employees</p>	<p>Identity card from employer and or employer letter is/are obtained only from corporate and other entities of repute, in addition to at least one of the officially valid documents of identification like, passport, PAN Card, voter identity Card, Driving Licence etc.</p>

Hindu Undivided Family account	<ul style="list-style-type: none"> i. Declaration from Karta, ii. Joint Hindu Family letter signed by the Karta and all major co-parceners. iii. PAN allotment letter for verification with a copy. iv. Telephone Bill for verification with a copy.
Account of Society, Association, Club, Schools & Colleges.	<ul style="list-style-type: none"> i. Certificate of Registration for verification with a copy certified by the Chairman/ Secretary, if registered. ii. Memorandum of Association (where applicable) certified by the Chairman/Secretary. iii. A copy of Resolution of Governing Body, Board of Directors or Managing Committee of the Society authorizing opening and operation of the account, certified by the Chairman of the meeting. iv. A list of Authorised signatories with their signatures attested by the Chairman/ Secretary. v. PAN allotment letter for verification with a copy. vi. Copy of Bye Laws, Rules, Regulations certified by the Chairman/Secretary. vii. Telephone Bill for verification with a copy.
Trust Accounts	<ul style="list-style-type: none"> i. Certificate of Registration for verification with a copy certified by the Chairman.(for public Charitable trust). ii. Trust Deed for verification with a copy certified by the Chairman. (The deed should empower the trustees to open Bank account) iii. Resolution for opening and operating the account signed by all the Trustees. iv. Any document listing the names of the trustees/settlers/beneficiaries. v. A list of the names of trustees with their signatures attested by the Chairman. vi. PAN Allotment letter for verification with a copy. vii. Telephone bill for verification with a copy.

Annexure- II
Risk Categorisation

**List of Low/Medium/High risk Customers based on the recommendations of
IBA Working Group.**

APPENDIX – A

Low Risk	Medium Risk	High Risk
1. Cooperative Bank	1. Gas Station	1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN1267
2. Ex-staff, Govt./ Semi Govt. Employees	2. Car / Boat / Plane Dealership	2. Individuals or entities listed in the schedule to the order under Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.
3. Illiterate	3. Electronics (wholesale)	3. Individuals and entities in watch lists issued by Interpol and other similar international organizations.
4. Individual	4. Travel agency	4. Customers with dubious reputation as per public information available or commercially available watch lists.
5. Local Authority	5. Used car sales	5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.
6. Other Banks	6. Telemarketers	6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the Customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
7. Pensioner	7. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center	7. Customers based in high risk countries/jurisdictions or locations (refer Appendix C).
8. Proprietor- ship	8. Dot-com company or internet business	8. Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
9. Public Ltd.	9. Pawnshops	9. Non-resident Customers and foreign nationals.

10. Public Sector	10. Auctioneers	10. Embassies / Consulates.
11. Public Sector Bank	11. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.	11. Off-shore(foreign) corporation/ business .
12. Staff.	12. Sole Practitioners or Law Firms (small, little known)	12. Non face-to-face Customers
13. Regional Rural Banks	13. Notaries (small, little known)	13. High net worth individuals
14. Govt./Semi- Govt. Local Body	14. Secretarial Firms (small, little known)	14. Firms with 'sleeping partners'
15. Cooperative Society	15. Accountants(small, little known firms)	15. Companies having close family shareholding or beneficial ownership
16. Senior Citizens	16. Venturecapital companies	16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
17. Self Help Groups	17. Blind	17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
	18. Purdanashin.	18. Investment Management / Money Management Company/Personal Investment Company.
	19. Registered Body.	19. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.
	20. Corporate Body	20. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies).
	21. Joint Sector	21. Money Service Business: including seller of: Money Orders / Travelers' Cheques / Money Transmission / Cheque Cashing / Currency Dealing or Exchange.
	22. Partnership	22. Business accepting third party cheques (except supermarkets or retail stores that accept payroll

		cheques/cash payroll cheques)
	23. Private Bank	23. Gambling/gaming including "Junket Operators" arranging gambling tours.
	24. Private Ltd. Company	24. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
	25. Unregistered body.	25. Customers engaged in a business which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries).
		26. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
		27. Customers that may appear to be Multi level marketing companies etc.
		28. Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence).
		29. Associations/Clubs
		30. Foreign Nationals.
		31. NGO.
		32. Overseas Corporate Bodies.
		33. Bullion dealers and Jewelers (subject to enhanced due diligence)
		34. Pooled accounts.
		35. Other Cash Intensive business.
		36. Shell Banks – Transactions in corresponding banking.
		37. Non face to face customer.
		38. Non-Bank Financial Institution
		39. Stock brokerage
		40. Import / Export
		41. Executors/Administrators
		42. HUF.
		43. Minor.

The above categorization of customers under risk perception is only illustrative and not exhaustive.

Risk Categorization of customers based on various parameters

Table – II

Basis	High Risk	Medium Risk	Low Risk
Type of Customer	(i) Private Ltd., Company	(i) Public Ltd companies (widely held)	(i) Salaried persons.
	(ii) Public Ltd Company (Closely held)	(ii) NRIs with balance of Rs.25 lakhs and above, but < Rs.50 lakhs.	(ii) Pensioners
	(iii) Trusts	(iii) Firms with sleeping partners.	(iii) Professional & Self employed persons.
	(iv) Charities		(iv) Agriculturist
	(v) NRIs having aggregate deposit of Rs.50 lakhs & above		(v) Self Help Groups
	(vi) Politically Exposed Persons		(vi) Government companies.
	(vii) Non-Face to face customers with aggregate deposit of Rs.10 lakhs and above.		(vii) Public Sector companies.
	(viii) Customers having adverse publicity.		(viii) Government Departments.
	ix) NRIs of Indian Origin.		(ix) NRIs with balance of less than Rs.25 lakhs and below.
	(ix) Firms with operative transactions authorized by sleeping partner.		
Source (Nationality) of Funds	Foreign Remittances from national of Gulf, Pakistan, Afghanistan, Libya and Syria	Foreign Remittance from national of Eastern Block Countries, Indonesia, Burma, Malaysia, Singapore and Thailand	Foreign Remittance nationals of United States and European Countries. Foreign Remittances from NRIs & persons of Indian origin.
Location of Customer	Developing Countries, African Countries, South American Countries	Asian Countries, Russia and China.	United States and European Countries.

Quantum of Transaction	Cash transaction of Rs. 5 lakh and above. Non cash transactions of Rs.10 lakhs and above <u>One time transaction</u> Rs. 1 lakh and above (cash.) Rs.5 lakh and above (non cash)	Cash transaction of Rs. 1 lakh & above but less than 5 lakhs. Non cash transactions of Rs.2 lakhs & above but below Rs.10 lac. <u>One time transaction</u> Rs. 20,000 and above but below 1 lakh cash Rs.1 lakh and above but less than Rs.5 but less than Rs.5 lakhs (non cash)	Cash transactions less than Rs. 1 lakh. Non cash transactions Less than Rs.2.00 lakhs. <u>One time transaction</u> Less than Rs.20,000/- Cash Less than Rs.1 lakhs non cash
Business Activity	(1) Jewellery	(i) Commodity Trade	(i) Industry
	(2) Chit Funds	(ii) S M Es with annual turnover Rs. 10 Crores and above, but < Rs.25 Crores	(ii) Hotel
	(3) Finance Companies.		(iii) Plantations
	(4) Foreign Exchange, Money Market Brokers		(iv) S M Es with turnover less than Rs. 10 Crores.
	(5) Travel Agencies		(v) Retail Trade
	(6) Export/ Import Trade		
	(7) S M Es with annual turnover exceeding Rs. 25 Crores and above.		
Composition of partners, directors	Entirely Foreign nationality	A mix of Indian and Foreign nationals	Exclusively Indian nationals

Annexure- iii

CONNECTED CASH TRANSACTIONS

The following transactions have taken place in a branch during the month of April,2013

Date	Mode	Dr (in Rs.)	Cr (in Rs.)	Balance (inRs.) BF- 8,00,000.00
02/04/2013	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2013	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2013	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		10,10,000.00	6,00,000.00	

- i) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs.10 lakhs. However, the bank should report only the debit transaction taken place on 02/04 & 08/04/2013. The debit transaction dated 07/04/2013 should not be separately reported by the bank, which is less than Rs.50,000/-.
- ii) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2013 should not be reported by banks.

Annexure-iv

LIST OF SUSPICIOUS ACTIVITIES

A) Transactions Involving Large Amounts of Cash:

- i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
- i. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
- ii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
- iii. Frequent withdrawal of large amounts of cash that do not appear to be justified by the customer's business activity;
- iv. Large cash withdrawals from a previously dormant / inactive account, or from an account which has just received an unexpected large credit from abroad;
- v. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the Company, e.g. cheques, letters of credit, bills of exchange etc.;
- vi. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

B) Transactions that do not make Economic Sense:

- (i) A customer having a large number of accounts with the same bank, with frequent transfer between different accounts;
- (ii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

C) Activities not consistent with the Customer's Business:

- i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques
- ii. Corporate accounts where deposits & withdrawals by cheque / telegraphic transfers foreign inward remittances / any other means are received from / made to sources apparently unconnected with the corporate business activity / dealings.
- iii. Unusual applications for DD/TT/PO against cash.
- iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
- v. Retail deposit of many cheques but rare withdrawals for daily operations.

D) Attempts to avoid Reporting / Records – Keeping requirements:

- i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- ii. Any individual or group that coerces / induces or attempts to coerce / induce a bank employee not to file any reports or any other forms.
- iii. An account where there are several cash deposits / withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E) Unusual Activities:

- i. An account of a customer who does not reside / have office near the branch even though there are bank branches near his residence / office.
- ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.

- iii. Funds coming from the list of countries / centers which are known for money laundering.

F) Customer who provides Insufficient or Suspicious Information:

- i. Sending or receiving frequent or large volumes of remittances to / from countries outside India.
- ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account / center on the same day leaving minimum balance in the account.
- iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire / funds transfer.

G) Certain Bank Employees arousing Suspicion:

- i. An employee whose lavish lifestyle cannot be supported by his or her salary.
- ii. Negligence of employees / willful blindness is reported repeatedly.

H) Some examples of suspicious activities / transactions to be monitored by the operating staff:

- i. Large Cash Transactions
- ii. Multiple accounts under the same name
- iii. Frequently converting large amounts of currency from small to large denomination notes
- iv. Placing funds in term Deposits and using them as security for more loans.
- v. Large deposits immediately followed by wire transfers.
- vi. Sudden surge in activity level .
- vii. Same funds being moved repeatedly among several accounts.

- viii. Multiple deposits of money orders, Banker's cheques, drafts of third parties.
- ix. Transactions inconsistent with the purpose of the account .
- x. Maintaining a low or overdrawn balance with high activity.
- xi. Where there is no commercial rationale for the customer buying the product he seeks.
- xii. Requests for a complex or unusually large transaction which has no apparent economic or lawful purpose.
- xiii. Requests to associate undue levels of secrecy with a transaction.
- xiv. Situations where the origin of wealth and / or source of funds cannot be easily verified or where the audit trail has been deliberately broken and / or unnecessarily layered.
- xv. The unwillingness of customers who are not private individuals to give the names of their real owners and controllers.

I) Check list for preventing money-laundering activities:

- i. A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire / funds transfer originates or into which wire / funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- ii. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.

- iii. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- iv. A customer experience increased wire activity when previously there has been no regular wire activity.
- v. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- vi. A business customer uses or evidences or sudden increase in wired transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.
- vii. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- viii. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- ix. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- x. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.
- xi. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- xii. Periodic wire transfers from a person's account/s to Bank haven countries.
- xiii. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- xiv. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold or that involve numerous Bank or travellers cheques.

- xv. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
 - a) The amount is very large (say over Rs.10 lakhs)
 - b) The amount is just under a specified threshold
 - c) The funds come from a foreign country or
 - d) Such transactions occur repeatedly.
- xvi. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold).
- xvii. A Non customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

Annexure- v

LIST A – DOCUMENTS FOR IS A CHECK

	DOCUMENT	Identity check	Signature check	Address check
i)	PAN Card	Yes	Yes	No
ii)	Voter's ID card * (to be accepted with a self-signed cheque)	Yes	No	Yes
iii)	Driving license (to be accepted with a self-signed cheque)	Yes	No	Yes
iv)	Defense ID/Govt. ID/Indian post ID	Yes	Yes	No
v)	Employees ID Card card is not there then 'letter of Introduction' from HR dept or any authorized Signatory to sign on Company letter head – certifying	Yes	Yes	No
vii)	Photo Credit Card	Yes	Yes	No

Annexure-vi

LIST B – DOCUMENTS FOR ADDRESS CHECK

	Documents	Identity check	Signature check	Address check
i)	Latest existing Bank account statement or Bank passbook, where address is mentioned	No	No	Yes
ii)	Ration Card	No	No	Yes
iii)	Latest Credit Card statement	No	No	Yes
iv)	Latest Electricity Bill	No	No	Yes
v)	Latest Telephone Bill	No	No	Yes
vi)	Latest Copy of LIC or Insurance Premium receipt	No	No	Yes
vii)	Letter from employer certifying the current mailing address only from private limited and public limited companies	No	No	Yes
viii)	Existing valid house registered lease agreement on stamp paper(in case of rented / leased accommodation or shifting / transfer of residence)	No	No	Yes

The validity of the documents given in List B above should not be more than 3months.