KYC/AML/CFT Policy 2015

Subject – Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under PMLA, 2002

INDEX

1. INTRODUCTION

1.1 Bank has in place a policy on KNOW YOUR CUSTOMER (KYC) norms and ANTI MONEY LAUNDERING (AML) measures approved by the Board in its meeting dated 29.10.2013. The policy was based on then guidelines issued by RBI.

1.2 The KYC guidelines have regularly been revisited by RBI in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) and has advised banks to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority.

1.3 RBI has advised banks to put in place a policy on 'Know Your Customer' and Anti-Money Laundering measures including the above referred recommendations with the approval of the Board.

1.4 RBI has issued the guidelines under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 and any contravention thereof or non-compliance may attract penalties under Banking Regulation Act.

1.5 This policy has been compiled taking into account covering the guidelines issued by RBI up to December 2014.

2. OBJECTIVES OF THE POLICY

2.1 To lay down policy framework for abiding by the Know Your Customer Norms and Anti Money Laundering Measure as set out by Reserve Bank of India, based on the recommendations of the Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.

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

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

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

2.5 To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.

3. SCOPE OF THE POLICY

3.1 This policy is applicable across all branches of the Bank, and is to be read in conjunction with related operational guidelines issued from time to time.

3.2 The contents of the policy shall be subject to the changes / modifications which may be advised by RBI and / or by any regulators and / or by Bank from time to time.

4. DEFINITIONS

4.1 Definition of Customer

For the purpose of KYC policy, a 'Customer' means -

I. a person or entity that maintains an account and / or has a business relationship with the Bank;
II. one on whose behalf the account is maintained (i.e. the beneficial owner).- 'Beneficial Owner' means the natural person who ultimately owns or controls a client and / or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person
III. beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
IV. any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

4.2 Definition of Beneficial Owner

The "beneficial owner" is 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.

Procedure for determining beneficial owner:

1. In case of a client who is not an individual or trust (i.e. company, partnership firm, unincorporated association or body of individuals), the beneficial owners of the client shall be identified through the identity of –

   (i) the natural person, who, whether acting alone or together, or through one or more judicial person, exercises control through ownership or who ultimately has a controlling ownership interest;
   (ii) the natural person exercising control over the juridical person through other means such as through voting rights, agreement, arrangements, etc., 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,
   (iii) the relevant natural person who holds the position of senior managing official, where no natural person is identified under (i) or (ii) above.

   Controlling ownership interest means -

   I. ownership of / entitlement to more than 25 percent of shares or capital or profits of the juridical person, where the juridical person is a company;
   II. ownership of / entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or,
   III. 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.

2. Where the client is a trust, the beneficial owners of the client shall be identified 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.

3. 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.

4. beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

5. 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.

4.3 Definition of Small Account

A 'small account' means a savings account where-

1. the aggregate of all credits in a financial year does not exceed rupees one lakh;
2. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
3. the balance at any point of time does not exceed rupees fifty thousand

In our bank we are having following products under 'small account'

Under Basic Savings Bank Deposit Account (BSBDA) –Relaxed KYC category

a) SB-Maha Bank Lok Bachat Yojana
b) FI-Maha Bank Lok Bachat Yojana
c) SB-Maha Setu-FI-W/o Cheq-Pub_Ind

Under Basic Savings Bank Deposit Account (BSBDA) –Complete KYC category

a) SB FI Maha Bank Scholaship Minority
b) Maha Sarvajan Saving Bank Deposit Account

4.4 Definition of High Net worth Individuals (HNIs)

Customers with any of the following shall be treated as High Net Worth Individuals;

1. Average balance exceeding Rs. 25 lakh in SB.
2. Average Balance exceeding Rs. 50 lakh in CA.
3. Term deposits exceeding Rs. 50 lakh in aggregate.
4. Annual turnover exceeding Rs. 25 lakh in the SB account, and exceeding Rs. 100 lakh in the CA account.
5. VIPs such as head of Village / Town / City, Top Executives of Companies etc.

For arriving at average balance in Savings and Current account, average balance during the immediately preceding last half financial year shall be considered.

For term deposits, aggregate term deposits of the customer at any point of time during the current financial year shall be considered.

4.5 Definition of *Walk-in Customers*

Walk-in-Customer means a Customer desirous of carrying out a transaction with our bank without having account with us. Transaction by walk-in-customers may be in the form of purchase of DD, NEFT/RTGS Remittance, purchase of third-party products such as insurance policies, mutual funds etc.

4.6 Definition of *Politically Exposed Persons (PEPs)*

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.

4.7 Definition of Non Face-To-Face Customers

Customers with whom the bank has not had direct interaction at the time of opening the account are considered as Non Fact-To-Face Customers.

5. Key Elements of KYC Policy

KYC policy of the bank has following four key elements;

i) Customer Acceptance Policy,
ii) Customer Identification Procedures,
iii) Monitoring of Transactions, and
iv) Risk Management.

5.1 Customer Acceptance Policy (CAP)

The criteria for acceptance of customers and the guidelines to be followed in this respect are as under:

5.1.1 No account shall be opened in anonymous or fictitious / benami name or on behalf of other persons whose identity has not been disclosed or cannot be verified.

5.1.2 'Small account' shall be opened on the basis of a self-attested photograph and affixation of signature or thumb print. Such accounts shall be opened and operated subject to the following conditions:

a. the designated officer of the branch, while opening the small account, shall certify under his / her signature that the person opening the account has affixed his / her signature or thumb print, as the case may be, in his / her presence;
b. It shall be ensured that foreign remittances are not credited to the account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;
c. A small 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 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;

d. A small 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"; and
e. Foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of "officially valid documents".

5.1.3 Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions / guidelines issued by Reserve Bank from time to time.

The information collected from the customer for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for cross selling or any other like purposes. Only that information shall be sought from the customer which is relevant to the perceived risk, is in conformity with the guidelines issued in this regard and is not intrusive, and. **Any other information from the customer shall be sought separately with his / her consent and after opening the account.**

A list of the nature and type of documents/information that shall be relied upon for customer identification is given in Annexure-I.

5.1.4 **At the time of opening of the account, the branch should obtain -**

a) "Officially Valid Documents" as applicable as per the category of the customer
b) 2 passport sized recent photographs for affixing them to the account opening form and specimen signature card/pass book.
c) specimen signature of the customer in the presence of a verifying official.
d) Instructions of the customers regarding mode of operation.
e) nomination in case of individual accounts, if not specifically refused the facility by the customer
f) details of accounts of the customer with other bank/s (if any)
g) Permanent Account Number (PAN) of the customer given by Income Tax authorities or declarations as applicable. Online verification of PAN number should be done.

Copies of the submitted KYC documents must be verified with the originals and officials accepting such documents should invariably put a stamp "Verified with the original(s)" under his/her signature and date.

The above documents/data would help to establish the identity of the person opening the account. However, for preparing risk profile of the customer, some additional details may be required such as business / employment details, source of income, annual income, assets owned, personal details such as qualification, marital status, etc. As already mentioned above, such additional information shall however be sought which is relevant to the perceived risk, is in conformity with the guidelines issued in this regard and is not intrusive. Besides, such additional information **shall be sought separately with his / her consent and after opening the account.**

5.1.5 No account shall be opened where the branch is unable to apply appropriate customer due diligence measures i.e. branch is unable to verify the identity and / or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data / information furnished to the branch.

Branches should also consider closing existing accounts under similar situations. **Decision for closure of the such accounts shall be taken at Zonal Office level and such account shall be closed only after obtaining approval of Zonal Office and also after giving due notice to the customer explaining the reasons for such a decision**.

5.1.6 **Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions, branches should not insist on introduction for opening bank accounts of customers, when documents of identity & address, as required, are provided.**

5.1.7 Under following circumstances / occasions, a customer shall be permitted to act on behalf of another person / entity, an account shall be permitted to be operated by a mandate holder or permitted to be opened by an intermediary in fiduciary capacity;

a) Accounts operated by power of attorney holders on the strength of duly registered PA wherein identity of the PA holder is verified by the bank.
b) Accounts operated as per mandate of the account holder, who has tendered the mandate before the bank officials and wherein identity of the mandate holder is verified by the bank.

5.1.8 Before opening a new account, branch should 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.

5.1.9 <u>Risk Categorization</u>

Branches should categorize every customer into any of the following three categories;

a) Low Risk
b) Medium Risk
c) High Risk

For categorization of the customer, branch should prepare a profile for each new customer which shall contain information relating to customer's identity, location, social / financial status, nature of business activity, mode of payments, volume of turnover, his clients' business and their location etc. However, while preparing customer profile, only such information shall be sought from the customer, which is relevant to the risk category.

5.1.9.1 **Low Risk Customers**

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

In case of low risk customers, only the basic requirements of verifying the identity and location of the customer shall be met.

In case a customer categorized as low risk is unable to submit the KYC documents due to genuine reasons, she/he shall submit the documents to the branch within a period of six months from the date of opening account.

5.1.9.2 **Medium Risk Customers**

Customers that are likely to pose a higher than average risk but lower than high risk to the bank shall be categorized as medium risk.

5.1.9.3 **High Risk Customers**

Customers especially those engaged in cash intensive businesses and for whom the sources of funds are not clear and who are likely to pose a higher risk to the bank shall be categorized as high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.

Bank shall apply enhanced and intensive 'due diligence' measures for high risk customers.

For illustrative examples of Low, Medium and High Risk customers, refer Annexure II. The list is however 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.

Bank shall adopt combination of automatic and manual classification of customers for risk categorization, based on the availability of data in CBS. Bank shall undertake system-generated risk categorization on the basis of data fields available in the system on half yearly basis. 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.

Risk Categorization of customers shall be based on combination of all the applicable parameters. Among the applicable parameters, highest risk grade will be assigned as overall Risk for the customer.

Periodical review of risk categorization of customers shall be undertaken once in every six months. Such review for the first half of the financial year i.e. April to September shall be undertaken in succeeding November, and for the second half the financial year i.e. October to March in succeeding May in every financial year.

5.1.10 In addition to what has been indicated above, bank shall take steps to identify and assess its Money Laundering (ML) / Terrorist Financial (TF) risk for customers, countries and geographical areas as also for products/ services/transactions/delivery channels. In this regard, bank shall use for guidance in our own risk assessment, the Report on Parameters for Risk-Based Transaction Monitoring (RBTM) issued by Indian Bank Association as a supplement to the Guidance Note on Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) standards.

5.1.11 While implementing customer acceptance policy, branches should ensure that banking services are not denied to general public, especially to those who are financially or socially disadvantaged.

5.2 Customer Identification Procedure (CIP)

5.2.1 Customer Identification Procedure shall be carried out at different stages, i.e., while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity / veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information. Sufficient information necessary to establish the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship shall be obtained to the satisfaction of the bank. **A list of the nature and type of documents/information that shall be relied upon for customer identification is given in Annexure-I.**

5.2.2 For customers that are natural persons, the branch shall obtain sufficient identification data to verify the identity of the customer, his/her address / location, and also his/her recent photograph.

5.2.3 For customers that are legal persons or entities, the branch shall –

(i) Verify the legal status of the legal person / entity through proper and relevant documents;
(ii) Verify that any person purporting to act on behalf of the legal person / entity is so authorized and identify and verify the identity of that person;
(iii) Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person

5.2.4 **Unique Customer Identification Code (UCIC)**

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. UCIC helps the bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

In our Bank, CIF of the customer is the Unique Number for that customer and it serves the purpose of Unique Customer Identification Code (UCIC).

Before creating a new CIF for any customer for opening any new account, branch should first verify that the same customer has not an existing CIF in the CBS system. If a customer has already been allotted a CIF, the new account(s) must be opened under the existing CIF only. No separate CIF should be created for him/her. For finding out the existing CIFs of all existing customers, "CIF-de-duplication" utility is provided under Intranet to the branches, which must be used before opening any new account for any customer.

Utility for knowing the customers already having multiple CIFs in the system is also provided to the branches. Branches should check up the reports provided under this utility on daily basis and undertake the exercise of keeping only one CIF for one customer by linking of additional CIFs created in the system for the same customer to a single CIF and deactivating all other CIFs.

5.2.5 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, full scale customer due diligence (CDD) shall be carried out before opening an account.

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

5.2.6 Officially Valid Documents

As per RBI's revised guidelines dated 17.07.2014, documents spelt out as "Officially Valid Documents" shall only be accepted for opening of new account. **No discretion to accept any other document for the account opening purpose shall be exercised by the branch official/s.** List of Officially Vaild documents required for opening of accounts is given in Annexure – I**. It is implied that proof of address also follows from the "Officially Valid Document" only.**

The information containing personal details like name, address, age, gender, etc., and photographs made available from UIDAI as a result of e-KYC process can also be treated as an 'Officially Valid Document'.

Branch shall obtain only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months. In case the proof of address furnished by the customer is not the local

address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence / local address. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

There is now no requirement of submitting two separate documents for proof of identity and proof of address. If the officially valid document submitted for opening a bank account has both, identity and address of the person, there is no need for submitting any other documentary proof.

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 shall be accepted as a valid proof of both identity and address.

If the current address is different from the address mentioned in the "Officially Valid Document" submitted by the customer, a simple declaration by him / her about his / her current address shall be obtained, for which no separate proof of address shall be required.

5.2.7 Branch should verify the genuineness of "Officially Valid Document/s" (including PAN Card) submitted by customer while opening / activating of account and /or effecting the transactions.

5.2.8. KYC verification of all the members of Self Help Groups (SHGs) is not required while opening the savings bank account of the SHG and KYC verification of only the officials of the SHGs would suffice. No separate KYC verification is needed at the time of credit linking the SHG.

5.2.9 ***Officially Valid Documents under Government of India notifications***

(a) Job card issued by NREGA duly signed by an officer of the State Government and the letters issued by the Unique Identification Authority of India ((UIDAI) containing details of name, address and Aadhaar number can now be accepted as an 'Officially Valid Document'.

(b) E-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process shall be treated as an 'Officially Valid Document'. However, the individual user has to authorize to UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches / business correspondents.

(c) Further, e-Aadhaar downloaded from UIDAI website shall be accepted as an officially valid document subject to the following :

i. If the prospective customer knows only his/her Aadhaar number, the branch shall print the prospective customer's e-Aadhaar letter in the branch directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above.

ii. If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the branch shall print the prospective

customer's e-Aadhaar letter in the branch directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

5.2.10 Opening of fresh accounts by customer shall not be insisted for inter-branch transfer of accounts by the customers. KYC once done by one branch shall be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer shall be allowed to transfer his account from one branch to another branch without restrictions. Existing account at the transferor branch shall be transferred 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.

5.2.11 If an existing KYC compliant customer of a bank desires to open another account in same or another branch of our bank, he / she need not submit fresh proof of identity and / or proof of address for the purpose.

5.2.12 Periodical updation of KYC

Periodical updation of KYC information of every customer shall be carried out in the following manner;

i) Full KYC exercise shall be done every **two years** for high risk customers, every **eight years** for medium risk customers and every **ten years** for low risk customers. Full KYC shall include all measures for confirming identity and address and other particulars of the customer that the branch may consider reasonable and necessary based on the risk profile of the customer.

Branch shall not insist on physical presence of low risk customer at the time of periodic updation.

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

Fresh photographs shall be obtained from minor customer on becoming major.

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

Such verification shall be done irrespective of whether the account has been transferred from one branch to another.

5.2.13 As regards non-compliance of KYC requirements by the customers despite repeated reminders by the branch, 'partial freezing' on such KYC non-compliant accounts shall be imposed in a phased manner. Branch shall exercise of option of imposing 'partial freezing', only after issuing due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. Thereafter, branch shall impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of

imposing initial 'partial freezing', branch shall disallow all debits and credits from / to the accounts, rendering them inoperative. Further, it would always be open to the bank to close the account of such customers. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force.

The sanctioning authority to approve the partial freezing, rendering the account inoperative and closure of such KYC non-compliant account will be as follows:

Category of Branch	Sanctioning Authority
Small, Medium, Large	Chief Manager/Assistant General Manager at Zonal Office Concerned
Very Large, Exceptionally Large	Deputy Zonal Manager (second in Command / Zonal Manager at Zonal Office concerned

5.2.14 **Customer Identification Requirements - Indicative Guidelines**

a) ***Walk-in Customers***

Where the amount of transaction is equal to or exceeds Rs.50000/-, it is necessary to obtain KYC documents (i.e. Officially Valid Documents in proof of identity and address) from a walk-in-customer and to verify the same by the authorized official of the bank.

As per our extant guidelines, no transaction of Rs.50,000/- and above is allowed to a non-customer against cash or otherwise, except in case of direct tax collection.

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 Rs. 50000/-, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address shall be verified. However, 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.50000/- the branch shall verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

However, in case of for all international money transfer operations, branches should verify the identity of every such customer.

b) ***Salaried Employees***

In case of salaried employees, branches should rely on certificate / letter of identity and / or address issued only from corporate and other entities of repute. It should however be verified whether the person issuing such certificate / letter of identity is the competent authority designated by the concerned employer to issue such certificate / letter. Further, in addition to the certificate / letter issued by the employer, branches should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving license, PAN Card, Voter's Identity card, etc.) for KYC purposes for opening bank accounts of salaried employees of corporate and other entities.

c) ***Trust / Nominee or Fiduciary Accounts***

There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Branch shall determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, shall be insisted on, as also details of the nature of the trust or other arrangements in place shall be obtained.

While opening an account for a trust, branches 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.

d) ***Accounts of companies and firms***

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with branches. Branches 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 shall 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.

e) ***Client accounts opened by professional intermediaries***

(i) When the branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branch shall hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches also maintain '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 must be identified. Where such funds are co-mingled at the bank, the branch shall still look through to the beneficial owners. Where the branch rely on the 'customer due diligence' (CDD) done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the branch.

(ii) 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. Bank shall 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.

f) ***Accounts of Politically Exposed Persons (PEPs) resident outside India***

i) Branches 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. Branches shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. **The decision to open an account for PEP shall be taken at Zonal office level by the Zonal Head.** Such accounts shall be subject to enhanced monitoring on an ongoing basis. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

ii) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, branch shall obtain approval from respective Zonal Office to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

iii) Zonal Offices shall closely monitor these types of accounts on ongoing basis for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

g) ***Accounts of non-face to face customers***

With the introduction of telephone and electronic banking, increasingly accounts are being opened by branches for customers without the need for the customer to visit the branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, certification of all the documents presented shall be insisted upon (e.g. Certification by independent authority such as notary, foreign resident banks, correspondent banking partners, embassy officials etc.) and, if necessary, additional documents shall be called for to establish identity and address etc.. In such cases, branches should insist that the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank shall have to rely on third party certification / introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

h) ***Accounts of proprietary concerns***

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, branches shall call for and **verify any two of the following documents before opening of accounts** in the name of a proprietary concern:

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 & 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 in the name of the proprietary concern by the Central Government or State Government Authority / Department. Branches shall also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the 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 and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Any two of the above documents would suffice. These documents shall be in the name of the proprietary concern.

i) ***Procedure to be followed in respect of foreign students:***

Branches shall follow the following procedure for foreign students studying in India;

a. Branch shall open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.
b. Within a period of 30 days of opening the account, the foreign student should submit to the branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution. Branch shall not insist on the landlord visiting the branch for verification of rent documents. Alternative means of verification of local address shall be adopted by branches.
c. During the 30 days period, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs.50,000/-, pending verification of address.
d. On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.

e. **Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.**

j) Selling Third party products

When bank sells third party products as agent, the responsibility for ensuring compliance with KYC / AML / CFT regulations lies with the third party. However, to mitigate reputational risk to bank and to enable a holistic view of a customer's transactions, branches are advised as follows:

(a) Even while selling third party products as agents, branch shall verify the identity and address of the walk-in customer.
(b) Branch shall also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in paragraph 2.24 below.
(c) Bank's AML software shall capture, generate and analyse alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers.
(d) Sale of third party products by branches as agents to customers, including walk-in customers, for Rs.50,000 and above shall be (a) by debit to customers' account or against cheques and (b) obtention & verification of the PAN given by the account based as well as walk-in-customers. This instruction would also apply to sale of bank's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for Rs. 50,000/- and above.

k) **Due Diligence in correspondent banking relationship**

Arrangement with co-operative banks etc. wherein these banks open current accounts with our bank and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in-customers for facilitating their remittances and payments, shall be monitored and reviewed from time to time to assess the risks including credit risk and reputational risk arising there from. For this purpose, bank shall retain the right to verify the records maintained by the client cooperative bank / societies for compliance with the extant instructions on KYC and AML under such arrangements.

l) **Simplified KYC norms for Foreign Portfolio Investors (FPIs)**

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence / verification prescribed by SEBI through a Custodian / Intermediary regulated by SEBI. Such eligible / registered FPIs may approach us for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank would be required. For this purpose, bank shall rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the Rules.

m) **Operation of Bank Accounts & Money Mules**

(a) "Money Mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they shall be having complicity with the criminals.

(b) In a Money Mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules shall be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

(c) To minimize the operations of such mule accounts, branches shall follow the guidelines on opening of accounts and monitoring of transactions contained in this Master Circular. Branches shall strictly adhere to the guidelines on KYC / AML / CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

n) **Bank No Longer Knows the True Identity**

In the circumstances when bank believes that it would no longer be satisfied about true identity of the account holder, bank shall also file an STR with FIU-IND.

5.3 Monitoring of Transactions

5.3.1 Ongoing monitoring is an essential element of effective KYC procedures

Branches can effectively control and reduce the risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Branch shall pay special attention to -

(i) All complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

(ii) Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch.

(iii) Very high account turnover inconsistent with the size of the balance maintained shall indicate that funds are being 'washed' through the account.

(iv) High-risk accounts shall be subjected to intensified monitoring.

(v) Branches should closely monitor high value transactions in all accounts, taking note of the background of each customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

(vi) High risk associated with accounts of bullion dealers (including sub-dealers) & jewelers shall be taken into account to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit - India (FIU-IND).

(vii) **Review of risk categorization of customers shall be carried out once in six months**.

(viii) Branches should closely monitor the newly opened accounts in the initial 6 months of their opening and track the transactions not in line with the profile of the customer.

(ix) There have been increased instances of fictitious offers, where fraudsters are using RBI"s corporate logo/name or any other reputed company in their e-mail messages to convince the victims of the authenticity of the purported messages conveying lottery/prize winning. The fraudsters persuade victims into making initial payment in a specified bank account towards the charges for clearance of the prize money. Whenever such instances are noticed, branches should make all efforts to educate the customers and sensitize them over the issue.

(x) Wherever request is received for change in Mobile number, loss of SIM Card, complaints of sudden inactivation or failure of mobile connection, branch should subject such accounts to enhanced monitoring and multiple checks, including calling on such mobile number/land line number seeking confirmation through other modes like e-mail etc.

i. An illustrative checklist for preventing money laundering activities is as under :

(a) 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.)

(b) 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 of money.

(c) 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.

(d) 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.

(e) A customer experiences increased wire activity when previously there has been no regular wire activity.

(f) Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

(g) A business customer uses or evidences of 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.

(h) 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.

(i) Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

(j) Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

(k) Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

(l) Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

(m) Periodic wire transfers from a person's account/s to Bank haven countries.

(n) A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

(o) 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.

(p) 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 the amount is very large (say over Rs.10lakhs).

- The amount is just under a specified threshold (Rs.10lacs)
- The funds come from a foreign country or
- Such transactions occur repeatedly.

(q) A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Banker's cheques (just under a specified threshold)

(r) A non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

5.3.2 Customer-category-wise **threshold limits** for transactions (per day) in the accounts under different risk categories and product codes of deposit accounts as prescribed are given in Annexure IV.

The transactions taking place exceeding these limits shall be informed to the branches through a link / report on the next day. Branches should go through the report every day and ensure that the transactions taken place are in conformity with their understanding/knowledge of the customer and his/her activity, means and worth etc. Wherever necessary, branch should seek clarification from the

customer and get satisfied with the genuineness of the transaction. Transaction of suspicious nature should immediately be reported to Zonal Office / Inspection Department, H.O. (AML Cell) for seeking guidance on steps to be initiated.

5.3.3 **Accounts of MLM Companies**

It has observed that accounts of Multi-level Marketing (MLM) Companies were misused for defrauding public by luring them into depositing their money with the MLM company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM company's account from new depositors, the cheques are honoured but once the chain breaks, all such post-dated instruments are dishonoured. This results in fraud on the public and is a reputational risk for the Bank concerned. Branch shall closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheque books 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 branch shall carefully analyze such data and in case they find such unusual operations in accounts, the matter shall be immediately reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance.

5.3.4 **Branch 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.

5.3.5 **The risk categorization of customers** as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by branches are extremely important for effective implementation of KYC / AML / CFT measures. Branches shall ensure effective implementation of the Reserve Bank's guidelines in this area and compliance with the regulatory guidelines on KYC / AML / CFT both in letter and spirit, without any laxity to as to avoid vulnerability to operational risk.

5.4 **Risk Management**

5.4.1 Bank has put in place an effective KYC programme by establishing appropriate procedures and ensuring their effective implementation.

5.4.2 Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. 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 is being put up before the Audit Committee of the Board on quarterly intervals.

6. Introduction of New Technologies - Credit Cards / Debit Cards / Smart Cards /Gift Cards

Bank shall pay special attention to any money laundering threats that shall arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Bank is issuing a variety

of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. **Branches are required to ensure full compliance with all KYC / AML / CFT guidelines issued from time to time, before issuing cards in respect of the customers including add-on / supplementary cardholders. The agents through whom marketing of credit cards is done shall also be subjected to KYC measures.**

7. Combating Financing of Terrorism

In terms of PMLA Rules, suspicious transaction shall include, inter alia,

(a) Bank has developed suitable mechanism through appropriate policy framework for enhanced monitoring of transactions, which give rise to a reasonable ground of suspicion that these shall involve financing of the activities relating to terrorism, and .accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to 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, the Bank shall update the lists of individuals and entities as circulated by Reserve Bank. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

I. "Al-Qaida Sanctions List", which is maintained by the 1267 / 1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

II. "1988 Sanctions List", which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/committees/ 1988/list.shtml

Both "Al-Qaida Sanctions List" and "1988 Sanctions List" shall be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

Before opening any new account, branches shall ensure that the name/s of the proposed customer does not appear in the lists. Further, branch shall 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.

7.1 Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

7.1.1 The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in

terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

7.1.2 Branches shall strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex III) and ensure meticulous compliance to the Order issued by the Government.

7.1.3 On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, bank shall ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing / unfreezing of financial assets of the designated individuals / entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts.

7.1.4 As per the designated list of banks received from RBI in terms of Para 4 of the Order, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts, the Bank shall –

a. Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals / entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.
b. In case, the particulars of any of their customers match with the particulars of designated individuals / entities, the bank shall immediately, not later than 24 hours from the time of finding out such customer, 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 to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post shall necessarily be conveyed on e-mail id: jsis@nic.in
c. Bank shall also send by post, a copy of the communication mentioned in (ii) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Central Office, Reserve Bank of India, Anti Money Laundering Division, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai - 400 001 and also by fax at No.022-22701239. The particulars, apart from being sent by post / fax shall necessarily be conveyed on e-mail id: cgmaml@rbi.org.in
d. Bank shall also send a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state / UT where the account is held as the case shall be and to FIU-India.
e. In case, the match of any of the customers with the particulars of designated individuals / entities is beyond doubt, the bank would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post shall necessarily be conveyed on e-mail id: jsis@nic.in
f. Bank shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

7.1.5 Freezing of financial assets

a. On receipt of the particulars as mentioned in paragraph d(ii)) above, IS-I Division of 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 bank are the ones listed as designated individuals / entities and the funds, financial assets or economic resources or related services , reported by bank are held by the designated individuals / entities. This verification would be completed within a period not exceeding five working days from the date of receipt of such particulars.
b. 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 within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.
c. The order shall take place without prior notice to the designated individuals / entities.

7.1.6 Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

a. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.
b. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.
c. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals / entities.
d. Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to bank and the procedure as enumerated at paragraphs 2.18[(c), (d) and (e)] shall be followed.
e. The freezing orders shall take place without prior notice to the designated persons involved.

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

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned / held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank. The bank shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact

details given in paragraph (d)(ii) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as shall 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.

7.1.8 Communication of Orders under Section 51A of Unlawful Activities (Prevention) Act

All Orders under Section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all bank through RBI.

7.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) Bank is required to take into account risks arising from the deficiencies in AML / CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, (latest as on June 30, 2014, being our circular DBOD. AML.No.15245/14.01.001/2013-14 dated March 05, 2014) bank shall also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that bank shall also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

(b) Bank shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to Reserve Bank / other relevant authorities, on request.

8. Correspondent Banking and Shell Bank

(a) Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services shall include cash / funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Bank shall gather sufficient information to understand fully the nature of the business of the correspondent / respondent bank. Information on the other bank's management, major business activities, level of AML / CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory / supervisory framework in the correspondent's / respondent's country shall be of special relevance. Similarly, bank shall try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships shall be established only with the approval of the Board, in case the Boards of some bank wish to delegate the power to an administrative authority, they shall delegate the power to a committee headed by the Chairman / CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee shall invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is

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

(b) ***Correspondent relationship with a "Shell Bank"***

Bank shall refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell bank are not permitted to operate in India. Banks shall not enter into relationship with shell bank and before establishing correspondent relationship with any foreign institution, bank shall take appropriate measures to satisfy itself that the foreign respondent institution does not permit its accounts to be used by shell bank. Bank shall be extremely cautious while continuing relationships with correspondent bank located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Bank shall ensure that its respondent bank have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

9. Applicability to bank and subsidiaries outside India

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

10. Wire Transfer

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

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

i. Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary shall be the same person.
ii. Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It shall include any chain of wire transfers that has at least one cross-border element.
iii. Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It shall also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer shall be located in another country.
iv. The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

b) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from

having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and / or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, branches must ensure that all wire transfers are accompanied by the following information:

10.1 ***Cross-border wire transfers***

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

ii. Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

iii. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

iv. All transactions, whether these are for trade or non trade or merchant are to be reported to FIU-IND, if it involves cross border transfers and exceeds the threshold limit of Rupees Five lakhs. All cross border wire transfers of value more than Rs 5.00 lakhs or its equivalent in foreign currency, where either the origin or destination is in India needs to be reported to the Director FIU-IND every month, every month by 15th of succeeding month.

10.2 ***Domestic wire transfers***

i. 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.

ii. If a branch has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the branch must 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.

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

c) Exemptions

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

d) Role of Ordering, Intermediary and Beneficiary banks

i) ***Ordering Bank***

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

ii) ***Intermediary bank***

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

iii) ***Beneficiary bank***

A beneficiary bank shall have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information shall be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they shall be reported to the Financial Intelligence Unit-India. The beneficiary 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 beneficiary bank shall consider restricting or even terminating its business relationship with the ordering bank.

11. Designated Director and Principal Officer

a) ***Designated Director***

Banks are required to nominate a Director on their Boards as "Designated Director", as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules. Accordingly, our Bank has nominated Executive Director to ensure overall compliance. The name, designation and address of the Designated Director is communicated to the Director, Financial Intelligence Unit - India (FIU-IND).

b) ***Principal Officer***

Bank has designated Deputy General Manager, Inspection & Audit, Head Office as Principal Officer.

Bank shall ensure that the Principal Officer acts independently and report directly to the senior management or to the Board of Directors. Principal Officer is located at the head office of the Bank and shall be responsible for monitoring and reporting of all transactions 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.

Further, the role and responsibilities of the Principal Officer shall 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 form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organizations of value more than Rupees Ten Lakhs or its equivalent in foreign currency to FIU-IND. With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.

12. 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)

Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act ibid.

a) ***Maintenance of records of transactions***

Bank shall introduce a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

i. All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

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

Explanation - Integrally connected cash transactions referred to at (ii) above

The following transactions have taken place in a branch during the month of April 2008:

Date	Mode	Dr (in Rs.)	Cr (in Rs.)	Balance (in Rs.) BF - 8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		**10,10,000.00**	**6,00,000.00**	

iii. 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

iv. All transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]

v. All cash transactions where forged or counterfeit currency notes or banknotes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and
vi. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
vii. 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 & 08/04/2008 shall not be reported by bank.

(b) ***Information to be preserved***

Bank is required to maintain all necessary information in respect of transactions referred to in PML Rule 3 to permit reconstruction of individual transaction, including the following information:

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

(c) ***Maintenance and Preservation of Records***

i) Bank is required to maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 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, in terms of PML Amendment Act 2012 notified on February 15, 2013, bank shall maintain for at least five 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 five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification records and transaction data shall be made available to the competent authorities upon request.

iii) In paragraph 2.13 of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents / office records / memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at bank 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 are required to be preserved for ten years as is required under PMLA, 2002.

(d) ***Reporting to Financial Intelligence Unit – India***

i. In terms of the PMLA Rules, banks are 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:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri,
Website - http://fiuindia.gov.in/

Explanation : Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO). NPO means any entity or organization 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.

ii. The earlier prescribed multiple data files reporting format has been replaced by a new single XML file format. FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The OM issued on Reporting Formats under Project FINnet dated 31st March,2011 by FIU containing all relevant details are available on FIU's website. In this regard, a reference is also invited to circulars DBOD.AML.BC.No.39/14.01.001/2012-13 and DBOD.AML.BC.No.49/14.01.001/2012-13 dated September 7, 2012 and October 11, 2012 respectively. Accordingly, bank shall carefully go through all the reporting formats prescribed by FIU-IND.

iii. FIU-IND have placed on their website editable electronic utilities to enable banks to file electronic CTR / STR who are yet to install/adopt suitable technological tools for extracting CTR / STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank shall cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR / STR as have been made available by FIU-IND on their website http://fiuindia.gov.in. However, in case of our Bank, all the branches are computerized.

In terms of instructions contained in paragraph 2.3(b) of this Master Circular, branches are required to prepare a profile for each customer based on risk categorization. Further, vide paragraph 2.13(d), the need for periodical review of risk categorization has been emphasized. It is, therefore, reiterated that branches, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

13. Various Reporting Formats

a) ***Cash Transaction Report (CTR)***

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, bank shall scrupulously adhere to the following:

i. 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 their controlling offices shall, therefore, invariably be submitted on monthly basis (not on fortnightly basis) and bank shall ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

ii. 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 in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency Report - CCR). These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and shall be reported to FIU-IND in plain text form.

iii. While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

iv. 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.

v. A summary of cash transaction report for the bank as a whole shall be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted to FIU-India.

vi. In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, bank shall generate centralized Cash Transaction Reports (CTR) in respect of branches under core banking solution at one point for onward transmission to FIU-IND, provided:

a) The CTR is to be generated in the format prescribed by FIU-IND;
b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors / inspectors, when asked for; and
c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this Master Circular at Para 2.24 (a), (b) and (c) respectively are scrupulously followed by the bank.

However, in respect of branches not under CBS, the monthly CTR shall continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND. This is not applicable for our Bank as all our branches are under CBS.

b) ***Suspicious Transaction Reports (STR)***

i) While determining suspicious transactions, bank shall be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.

ii) It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. It is clarified that branches shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii) 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.

iv) The STR shall be furnished within seven 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. These STRs will be further approved by a Committee of 3 General Managers, and submitted to FIU-IND within 7 days of such approval from the Committee. Such report shall be made available to the competent authorities on request.

v) In the context of creating KYC / AML awareness among the staff and for generating alerts for suspicious transactions, banks shall consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, January 2012'. The Indicative List of Alert Indicators to report suspicious transactions / attempted transactions is enclosed at Annexure IV, and a list of Examples of STRs received at FIU-IND is also enclosed at Annexure–V.

vi) Bank shall not put any restrictions on operations in the accounts where an STR has been made. Bank and its employees shall keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It shall be ensured that there is no tipping off to the customer at any level.

(c) ***Non-Profit Organization***

The 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 submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format. Branches should mark “91” Code in Constitution Code in the CIF for identifying Non Profit Organizations’.

(d) ***Cross-border Wire Transfer***

Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India. Hence, all transactions, of value more than Rs. Five Lakhs, whether for trade or non trade or merchant, are to be reported to FIU-IND, if it involves cross border transfers.

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

a) ***Customer Education***

Implementation of KYC procedures require branches to demand certain information from customers which shall 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. There bank will prepare specific literature / pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

b) ***Employees' Training***

Bank will 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.

c) ***Hiring of Employees***

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

———

———

Annex – I

Customer Identification Procedure
Officially Valid Documents that shall be obtained from customers

Features		Documents
Accounts of individuals		
-	Normal Accounts	Any or more of the following which show/s both identity as well as address of the customer; (i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v) Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number (vii) Any document as notified by the Central Government in consultation with the regulator **It is implied that proof of address also follows from the above documents only.**
-	Simplified KYC for 'Low Risk Customers'	Any of the above and / or any of the following; (i) Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Bank and Public Financial Institution (ii) Letter issued by a gazette officer, with a duly attested photograph of the person.
Accounts of companies		(i) Certificate of incorporation (ii) Memorandum & Articles of Association (iii) A Resolution of the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf; and (iv) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf
Accounts of partnership firms		(i) Registration certificate (ii) Partnership deed (iii) An officially valid document in respect of the person holding an attorney to transact on its behalf.

Features	Documents
Accounts of trusts & foundations	(i) Registration Certificate (ii) Trust Deed; and (iii) An officially valid document in respect of the person holding a power of attorney to transact on its behalf.
Accounts of Unincorporated associations or body of individuals	(i) Resolution of the Managing Body of such association or body of individuals; (ii) Power of attorney granted to him to transact on its behalf; (iii) An officially valid document in respect of the person holding an attorney to transact on its behalf; and . (iv) Such information as may be required by the branch to collectively establish the legal existence of such an association or body of individuals.

ANNEXURE II

Illustrative list of Low / Medium / High risk customers

Low Risk Customers

1. Salaried employees whose salary structures are well defined
2. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
3. Government Departments and Government owned companies
4. Regulators and Statutory bodies, etc.
5. NPOs / NGOs only which are promoted by United Nations or its agencies

Medium Risk Customers

1. Non-Bank Financial Institution
2. Stock brokerage
3. Import / Export
4. Gas Station
5. Car / Boat / Plane Dealership
6. Electronics (wholesale)
7. Travel agency
8. Used car sales
9. Telemarketers
10. Providers of telecommunications service, internet cafe, IDD call service, phone cards, phone center
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers
14. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
15. Sole Practitioners or Law Firms (small, little known)
16. Notaries (small, little known)
17. Secretarial Firms (small, little known)
18. Accountants (small, little known firms)
19. Venture capital companies

High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.
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. Individuals and entities in watch lists issued by Interpol and other similar international organizations
4. Customers with dubious reputation as per public information available or commercially available watch lists
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
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. Customers based in high risk countries / jurisdictions or locations (Refer Annexure-III)
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. Non-resident customers and foreign nationals
10. Embassies / Consulates
11. Off-shore (foreign) corporation / business
12. Non face-to-face customers
13. High net worth individuals
14. Firms with 'sleeping partners'
15. Companies having close family shareholding or beneficial ownership
16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
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. Investment Management / Money Management Company / Personal Investment Company
19. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
21. 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)
22. Money Service Business: including seller of: Money Orders / Travelers' Checks / Money Transmission / Check Cashing / Currency Dealing or Exchange
23. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks / cash payroll checks)
24. Gambling / gaming including "Junket Operators" arranging gambling tours
25. 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).
26. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
28. Customers that may appear to be Multi level marketing companies etc.

ANNEXURE III

High risk countries / jurisdictions or locations;

Iran	Albania	Kuwait	Sudan
Democratic People's Republic of Korea (DPRK)	Angola	Lao PDR	Syria
Algeria	Argentina	Namibia	Tajikistan
Ecuador	Cambodia	Nicaragua	Turkey
Indonesia	Cuba	Pakistan	Uganda
Myanmar	Ethiopia	Panama	Yemen
Afghanistan	Iraq	Papua New Guinea	Zimbabwe

ANNEXURE IV					
Customer-Category-wise Threshold Limits for per transactions as per Risk Category of the customer, type of account / product code of the account					
ACCT TYPE	**Int _Cat**	**Description**	**Risk Category**		
			Low	**Medium**	**High**
SAVINGS					
2011	1401	SB-Chq General-Pub-IND-ALL	2,00,000	1,50,000	1,00,000
2011	2401	SB-ChqGeneral-Pub-Oth-All	2,00,000	1,50,000	1,00,000
2011	3401	SB-ChqGeneral-Staff-All	2,00,000	1,50,000	1,00,000
2011	6401	SB-ChqGeneral-Trust-All	xxxx	xxxx	1,50,000
2013	1401	SB-ChqNRO-Pub- Ind-AllINR	xxxx	xxxx	5,00,000
2014	1401	SB-ChqNRE-Pub- Ind-AllINR	xxxx	xxxx	5,00,000
2017	1401	Sav-Chq-FGN-Nat-Pub-Ind-AllINR	xxxx	xxxx	5,00,000
2020	1401	SB-ChqPENSNPub-Ind-AllINR	1,00,000	xxxx	xxxx
2020	3401	SB-ChqPENSNSTFFInd-AllINR	1,00,000	xxxx	xxxx
2022	1401	SB-Maha Bank Lok Bachat Yojana	10,000	xxxx	xxxx
2023	1401	Sav-Chq-Yuva-Pub-Ind-AllINR	50,000	xxxx	xxxx
2026	1401	SB-SalaryGain-Pub-Ind-All	1,00,000	xxxx	xxxx
2026	3401	SB-SalaryGain-STF-Ind-All	1,00,000	xxxx	xxxx
2029	1401	SB-Chq-Flexi -Pub- Ind-All-INR	2,00,000	xxxx	xxxx
2029	3401	SB-Chq-Flexi -Staff-All-INR	2,00,000	xxxx	xxxx
2030	3401	Sav-Chq-Flexi NRO-Stff-All-INR	xxxx	xxxx	10,00,000
2031	1401	Sav-Chq-Flexi-NRE-Pub-Ind-AlII	xxxx	xxxx	10,00,000
2033	1401	FI-Maha Bank Lok Bachat Yojana	10,000	xxxx	xxxx
2064	1401	MahaSurakshaPayroll-CommOff	2,00,000	xxxx	xxxx
2065	1401	MahaSurakshaPayrol-BelCommOff	2,00,000	xxxx	xxxx
2090	3401	SB-CO-Chq-Gen-St-All	2,00,000	xxxx	xxxx
2090	6401	SB-CO-Chq-Gen-Trust-All	xxxx	xxxx	1,00,000
2111	1401	SB-W/oChq-Gen-Pub-Ind-AllINR	2,00,000	1,50,000	1,00,000
2120	1401	SB-WChq-Pens-Pub-Ind-AllINR	1,00,000	xxxx	xxxx
2122	1401	SB-MahaSetu-FI-W/oCHq-Pub_Ind	10,000	xxxx	xxxx
2123	1401	SB-w/o-Chq-Bk-YUVA-INSTACARD	10,000	xxxx	xxxx
2124	1401	SB-NSIGSESchoI-W/oCHq-Pub_Ind	10,000	xxxx	xxxx
2125	1401	SB-CapitalGain-Pub-Ind-All-INR	10,00,000	7,50,000	5,00,000
2125	2401	SB-CapitalGain-Pub-Oth-All-INR	10,00,000	7,50,000	5,00,000
2129	1401	SB-w/oFlexi -Pub- Ind-All-INR	2,00,000	1,50,000	1,00,000
2133	1401	SBFIMahaBank Schlrshp Minority	10,000	xxxx	xxxx
2311	1401	Mahabank CorpSUP Payroll Schem	2,00,000	xxxx	xxxx
2353	2401	SBChqMahabank Govt Zero BalSch	10,00,000	xxxx	xxxx
2058	1401	Mahabank Royal SB A/C	10,00,000	7,50,000	5,00,000
2059	1401	Maha Sarvjan SB A/C	10,000	xxxx	xxxx
2091	1401	Mahabank Puple SB A/C	10,00,000	7,50,000	5,00,000

ACCT TYPE	Int _Cat	Description	Risk Category		
			Low	Medium	High
CURRENT					
1011	1101	Cur-Gen-Pub-Ind-NonRural-INR	10,00,000	7,50,000	5,00,000
1011	1991	Cur-Gen-Pub-Ind-Rural-SU-INR	7,00,000	5,00,000	3,00,000
1011	2101	Cur-Gen-Pub-Corp-NonRural	25,00,000	15,00,000	10,00,000
1011	2991	Cur-Gen-Pub-Corp-oth-Rural-SU	10,00,000	7,50,000	5,00,000
1011	6401	Cur-Gen-Trusts-All-INR	xxxx	xxxx	5,00,000
1053	2401	Cur-Govt-Pub-Oth-AllINR	10,00,000	xxxx	xxxx
1054	2101	BOM e-PAYMENT OF TAX	xxxx	xxxx	xxxx
1057	1401	Cur-Diamond Pub-Ind-INR	10,00,000	7,50,000	5,00,000
1057	2401	Cur-Diamond Pub-Oth-INR	10,00,000	7,50,000	5,00,000
1511	2101	CUR-SPL-PUB-CORP-OTH-NRural	10,00,000	7,50,000	5,00,000

ANNEXURE V

Indicative Alert Indicators for Branches/ Departments to report suspicious transactions / attempted transactions

ALERT INDICATOR			INDICATIVE RULE / SCENARIO
	CV – Customer Verification		
1.	CV 1.1	Customer left without opening account	Customer did not open account after being Informed about KYC
2.	CV.2.1	Customer offered false or forged identification documents	Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate
3.	CV2.2	Identity documents are not verifiable	Identity documents presented are not verifiable i.e. Foreign documents etc.
4.	CV3.1	Address found to be non existent	Address provided by the customer is found to be non-existent
5.	CV3.2	Address found to be wrong	Customer not staying at address provided during account opening
6.	CV4.1	Difficult to Identify beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
	LQ – Law Enforcement Agency Query		
7.	LQ1.1	Customer is being investigated for criminal offences	Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences
8.	LQ2.1 -	Customer is being investigated for TF offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities.
	MR – Media Reports		
9.	MR1.1	Adverse media report about criminal activities of customer	Match of customer details with persons reported in local media/ open source for criminal offences
10.	MR 2.1	Adverse media report about TF or terrorist activities of customer	Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities.

ALERT INDICATOR			INDICATIVE RULE / SCENARIO
	EI – Employee Initiated		
11.	EI 1.1	Customer did not complete transaction	Customer did not complete transaction after queries such source of funds etc.
12.	EI 2.1	Customer is nervous	Customer is hurried or nervous
13.	EI 2.2	Customer is over cautious	Customer over cautious in explaining genuineness of the transaction.
14.	EI 2.3	Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal, possibly false or inconsistent.
15.	EI 3.1	Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction. Customer taking instructions for conducting transactions. Customer is accompanied by unrelated individuals.
16.	EI 3.2	Multiple customers working as a group	Multiple customers arrive together but pretend to ignore each other
17.	EI 4.1	Customer avoiding nearer	Customer travels unexplained distances to conduct transactions
18.	EI 4.2 -	Customer offers different identifications on different occasions	Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.
19.	E14.3	Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting.
20.	E14.4	Customer could not explain source of funds	Customer could not explain source of funds satisfactorily .
21.	E15.1	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
22.	E15.2	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense 'for the particular customer.
23.	E15.3	Transaction inconsistent with business	Transaction involving movement of which is inconsistent with the customers business
24.	E16.1	Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA

ANNEXURE VI

Examples of STRs received At FIU-IND

S.N	Type of Suspicion	Summary of Detection and Report
1	False Identity	Identification documents found to be forged during customer verification process. The account holder not traceable.
2	Wrong Address	Welcome pack received back since the person was not staying at the given address. In some cases, the address details given by the account holder found to be false. The account holder not traceable.
3	Use of similar sounding corporate names	Account was opened with names very close to other established business entities.
4	Doubt over the real beneficiary of the account	Customer not aware of transactions in the account. Transactions inconsistent with customer's profile.
5	Account of persons under investigation	The customer reported in media for being under investigation/ Account of a customer frozen by the bank
6	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth/Father's name/Nationality) matched with details on a Watch List of UN, Interpol etc.
7	Account used for cyber crime	Complaints of cyber crime received against a customer. The transactions in the account have no valid explanation.
8	Account used for lottery fraud	Complaints received against a bank account used for getting money deposited by victims. No valid explanation for the transactions by account holder. Cash withdrawals using ATMs immediately after deposits.
9	Doubtful activity of account holder	Cash deposited in a bank account at multiple cities on the same day. The account holder a citizen of country with high rate of drug trafficking.
10	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
11	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economic rationale.
12	Unexplained activity in dormant accounts	The customer could not provide satisfactory explanation to transactions in a dormant account.
13	Suspicious cash withdrawals in bank account	Large value cheques deposited followed by immediate cash withdrawals.

S.N	Type of Suspicion	Summary of Detection and Report
14	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
15	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list
16	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list
17	Doubtful utilization of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation
18	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization
19	Unexplained activity in account inconsistent with what would be expected from declared business	Transactions in account inconsistent with declared business. The customer could not provide satisfactory explanation.
20	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account usually having small transactions without any economic rationale.
21	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
22	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
23	Doubtful use of safe deposit locker	Safe deposit locker operated frequently though the financial status of client does not warrant such frequency. Large suitcase brought by customer.
24	Doubtful source of cash deposited in bank account	Cash transactions of value just under the reporting threshold. Cash transactions spilt across accounts to avoid reporting. No valid explanation

ANNEXURE VII :

INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

i) Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the Institution to verify.

ii) Customer expressing unusual curiosity about secrecy of information involved in the transaction.

iii) Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.

iv) Customer giving confusing details about a transaction.

v) Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.

vi) Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.

ii) Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.

vii) Customer's representatives avoiding contact with the branch.

ix) Customers who repay the problem loans unexpectedly.

x) Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.

xi) Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.

xii) Customer regularly issues large value cheques without balance and then deposits cash.

xiii) Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions Involving Large Amounts of Cash

i) Exchanging an unusually large amount of small denomination notes for those of higher denomination;

ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

iii) Frequent withdrawal of large amounts by means of cheques, including traveler's cheques;

iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;

v) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;

vi) 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.;

vii) 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 transfers 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/Record-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 a 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) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
iii) A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain Suspicious Funds Transfer Activities

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.

H. 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.

I. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

i. 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) Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
ix) Cheques of third parties into the account followed by immediate cash withdrawals.
x) Transactions inconsistent with the purpose of the account.
xi) Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

a) 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).
b) 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.
c) 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.
d) 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.
e) A customer experiences increased wire activity when previously there has been no regular wire activity.
f) Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
g) A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
h) 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.
i) Sending or receiving frequent or large volumes of wire transfers to and from

offshore institutions.

j) Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

k) Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency

l) Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

m) Periodic wire transfers from a person's account/s to Bank haven countries.

n) A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

o) 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 travelers cheques

p) 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

q) The amount is very large (say over Rs.10 lakhs)

1. The amount is just under a specified threshold.

- The funds come from a foreign country or
- Such transactions occur repeatedly.

r) 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)

s) A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.