Policy Document on

Know Your Customer &

Anti Money Laundering Measures

(KYC & AML)

March 2013

The Karur Vysya Bank Limited
Inspection & Audit Department
Central Office,
Erode Road,
Karur

Policy Title	Know Your Customer Norms & Anti Money Laundering Measures
Version Number	KYCAML 4.0
Effective Date	31.03.2013
Initiated by	Inspection and Audit Department
Authorized by	Board
Last Revision Date	April 2012
Next Revision Date	April 2014
Policy Contains	50 Pages (Including cover Page)

1.0 Introduction

1.1 Money laundering has become a global menace threatening the stability of various regions by actively supporting and strengthening terrorist networks and criminal organizations. The links between money laundering, organized crime, drug trafficking and terrorism are not new and continue to threaten the stability of financial institutions and, ultimately, the democracy and the rule of law.

1.2 In common parlance, money laundering is thus the process by which, one conceals the existence of an illegal source or illegal application of income and then disguises that income to make it appear legitimate.

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

The 'Know Your Customer' (KYC) Policy is an important tool for combating money laundering.

2.0 Objectives of the Policy

- To enable the bank to know/understand the customers and their financial dealings better, which in turn would help the bank to manage risks prudently.
- To prevent criminal elements from using the bank for money laundering activities.
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- To comply with applicable laws and regulatory guidelines.
- To take necessary steps to ensure that the relevant staff are adequately informed and trained in KYC/AML procedures.

This policy is applicable to all our branches/offices and is to be read in conjunction with related operational guidelines issued from time to time.

3.0 Definitions

3.1 A "customer" for the purpose of this policy is defined as:

a) A person or an entity that maintains an account and/or has a business relationship with the bank.
b) iOne on whose behalf the account is maintained [i.e. the beneficial owner]
c) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
d) Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank.

3.2 Money laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the 'offence of money laundering' as under:

"Any person/entity who directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering".

3.2.1 Terrorist Financing

Terrorists use similar methods as Money Launderers for moving their funds. Some of the terrorist groups also indulge in criminal activities for generating funds for their activities and some of them are even known to have strong relationships with criminal gangs. The two major differences between terrorist financing and money laundering are:

a. Terrorist funding can happen from legitimately obtained income whereas the source of money in money laundering is. always from illegal source, and
b. More often terrorist activities require small amounts and hence it is increasingly difficult to identify terrorist funding transactions.

3.2.2 Other Financial Crimes

Other financial crimes such as Fraud and market abuse (insider trading) are closely related to money laundering and terrorist financing and most

often the measures 'described in these guidelines for preventing money laundering and terrorist financing may help financial institutions in preventing fraud and other financial Crimes, as well.

3.3 Obligations under Prevention of Money Laundering (PML) Act 2002

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

I. Maintaining a record of prescribed transactions
II. Furnishing information of prescribed transaction to the specified authority
III. Verifying and maintaining records of the identity of its clients
IV. Preserving records in respect of [i], [ii], [iii] above for a period of ten years from the date of cessation of transactions with the clients.

4.0 Key elements of the policy

- Customer acceptance policy (CAP)
- Customer identification procedures (CIP)
- Monitoring of transactions and
- Risk management

4.1 Customer Acceptance Policy (CAP)

Customers who satisfy the criteria laid down as under may open an account with our bank. A person or entity not eligible as per this policy shall not be allowed to open an account.

4.1.1 No account is opened in anonymous or fictitious/ benami name(s);

4.1.2 Branches have to classify the customers according to the risk perception based on the following:

- The nature of business activity,
- Location of customer and his clients,
- Mode of payments,
- Volume of turnover,
- Social and financial status etc

Branches have to categorize the customers into low, medium and high risk. Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorized as very high.

4.1.3 Documentation requirements and other information to 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;

4.1.4 Branches should not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. The branches should, however, avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after consulting the Divisional Head and giving due notice to the customer explaining the reasons for such a decision;

4.1.5 Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of the country / banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity

4.1.6 Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

4.1.7 Branches should carry out proper Customer Due Diligence based on the risk perception of the customer namely Basic and Simple Due Diligence for Low and Medium customers and Enhanced Due Diligence for high risk customers.

4.1.8 UIDAI system – KYC requirements

Additional communication received from RBI on this aspect to accept "Aadhar" as a valid document for KYC, if the address provided by the account holder is the same as that on Aadhar letter, it may be accepted as a proof of both identity and address.

4.1.9 Acceptance of NREGA Job Card as KYC for normal accounts

In terms of para 2.7 (B) (b) of RBI Master Circular, Accounts opened only on the basis of NREGA Job Card are subject to limitation applicable to 'Small Accounts' as prescribed in our circular DBOD.AML.No.77/

14.01.001/2010-11 dated January 27, 2011. In modification of instructions quoted above, banks are advised that they may now accept NREGA Job Card as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'.

4.2 Branches should prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile branches should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

4.3 Preparation of profile for each customer

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc.

In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank should be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Branches should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

Examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with ' sleeping partners '; (f) politically exposed persons (PEPs) of foreign origin; (g) non-face to face customers and (h) those with dubious

reputation as per public information available; (i) Bullion dealers (Including sub – dealers) & Jewelers etc. However, only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer.
The adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

5.0 Customer Identification Procedure (CIP)

5.1 The Customer Identification Procedure to 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 are as under:

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Branches have to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the branch must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the branches should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (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 authorised 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.

Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given

in paragraph 6.0 below for guidance of branches. If the branch decides to accept such accounts in terms of the Customer Acceptance Policy, the branch should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

5.2 It has been observed that some close relatives, e.g. wife, son, daughter and daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, branches can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Branches can use any supplementary evidence such as a letter received through post for further verification of the address. Branches should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

5.3 Branches should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The updation should be done as per the following guidelines:

i) Full KYC exercise will be required to be done at least every two years for high risk individuals and entities.

ii) Full KYC exercise will be required to be done at least every ten years for low risk and at least every eight years for medium risk individuals and entities.

iii) Positive confirmation (obtaining KYC related updates through e-mail/letter/telephonic conversations/forms/ interviews/visits, etc), will be required to be completed at least every two years for medium risk and at least every three years for low risk individuals and entities.

iv) iv)Fresh photographs will be required to be obtained from minor customer on becoming major.

5.4 An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annex-I. It is clarified that permanent correct address, as referred to, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the bank for verification of the address of the customer.

5.5 The indicative list furnished in Annex -I, should not be treated as an exhaustive list and as a result of which the public should not be denied access to banking services.

5.6 Introduction not Mandatory for opening accounts

Before implementation of the system of document-based verification of identity, as laid down in PML Act/Rules, introduction from an existing customer of the bank was considered necessary for opening of bank accounts. Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions, banks should not insist on introduction for opening bank accounts of customers.

5.7 Opening of new accounts – Proof of identity and address

In terms of RBI circular letter **DBOD.AML.BC. No. 65 /14.01.001/2012-13 dated 10.12.2012,** it has now been decided that for accepting a single document both for identity and address proof the following shall apply:

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

b) If the address indicated on the document submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address should be obtained. For this purpose, apart from the indicative documents listed in Annex I of the Master Circular, a rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

5.8 Shifting of Bank accounts to another centre – Proof of address

Banks were advised vide circular DBOD.AML.BC.No. 97/14.01.001/2011-12 dated April 27, 2012, that KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC had been done for the concerned account.

The customer should be allowed to transfer his account from one branch to another branch without restrictions. In order to comply with KYC requirements of correct address of the person, fresh address proof has to be obtained from him/her upon such transfer by the transferee branch.

However, a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a utility bill or other documents in their name as address proof immediately after relocating. In view of this, it has been decided that:

(a) Banks may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self- declaration from the account holder about his/her current address, subject to submitting proof of address within a period of six months.

(b) Banks may also accept rent agreement duly registered with State Government or similar registration authority indicating the address of the customer, in addition to other documents listed as proof of address in Annex I of our Master Circular on KYC/AML/CFT dated July 2, 2012.

6.0 Customer Identification Requirements – Indicative Guidelines

6.1 Trust/Nominee or Fiduciary Accounts

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

While opening an account for a trust, branches should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

6.2 Accounts of companies and firms

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with bank. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may

be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

6.3 Client accounts opened by professional intermediaries

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. Branches may 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 bank should still look through to the beneficial owners.

Where the branches rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the branch.

Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that branches should 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, should not be allowed to open an account on behalf of a client.

6.4 Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior

government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken by the Divisional Head under whose jurisdiction the branch falls. Branches should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs. The branches should collect such particulars from the PEP at the time of opening of the accounts.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, branches should obtain Divisional Office approval 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 a PEP is the ultimate beneficial owner.

Further, branches should follow appropriate ongoing risk management procedures 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.

6.5 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 bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, branches may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third

party is a regulated and supervised entity and has adequate KYC systems in place.

6.6 Walk in Customers.

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

6.7 Accounts of Proprietary concerns

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

a) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/license 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, License 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 documents issued by the Central Government or State Government Authority / Department, Importer Exporter Code (IEC) issued by the office of Directorate General of Foreign Trade (DGFT) , etc.

b) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

c) These guidelines on proprietorship concerns will apply to all new and existing customers.

6.8 Multi Level Marketing (MLM) firms

Special ongoing monitoring of the operations in the accounts of such types of firms should be made especially if large volumes of small cash deposits are being made in those accounts and withdrawals are being made there from, through cheques written for small amounts, either across the counters or through clearing. In respect of such account holders banks may, in specific cases, call for the data from the account holders on the number and aggregate amount of post dated cheques issued.

The data/information so collected should be analysed in select cases to rule out the possibility of the firms being engaged in deposit taking activities. Certain indicative parameters for selecting accounts for further scrutiny and action are the bunching of dates of the post dated cheques, the uniformity in the amounts of cheques, etc. These data should be analysed together with data on cash deposits of small amounts on previous distant dates resembling the deposit contracting/mobilisation dates in terms of similar bunching and uniformity of amounts. Any unusual operations noticed during the above review is required to be immediately reported to RBI and other appropriate authorities such as Financial Intelligence Unit (FIU-IND).

6.9 Opening of bank Accounts - salaried employees

For opening bank accounts of salaried employees some banks rely on a certificate/letter issued by the employer as the only KYC document for the purposes of certification of identity as well as address proof. Such a practice is open to misuse and fraught with risk. RBI has clarified that with a view to containing the risk of fraud banks need to rely on such certification only from corporates and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, in addition to the certificate from employer, banks 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.) or utility bills for KYC purposes for opening bank account of salaried employees of corporates and other entities.

6.10 Money Mules

Branches are advised to exercise due caution about operation of the bank account that are being. used as a "money mule" for purpose of

laundering money. The money mule can be used to launder the proceedings of frauds schemes (e.g. phishing, scam mails and identity thefts) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money Mules ".

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/entity, for a specified commission payment. Money' mules may be recruited through a variety of methods, including spam emails, advertisements on genuine recruitment websites, social networking sites, instant messaging and advertisements in newspapers. In some cases these third parties may be innocent while in others- they may be working jointly with fraudsters in duping general public.

A 'money mule' is .used typically when a fraudster needs, an account in which the illegally obtained/stolen funds are transferred and then funds are subsequently laundered. elsewhere. Many a times, the address and contact details of such mules are found to be fake or not updated making it difficult for enforcement agencies to locate the account holder.

In order to tackle the above misuse by money mules, Banks need to identify and report money mule accounts. Some of the indicators for Identifying money mule accounts could be accounts Where the customer always transacts through third parties', accounts where the Customer/beneficiary is not contactable or unwilling to meet or uncomfortable providing transaction related information and transactions which are not in line with the customer profile and business or accounts where complaints are received from customers/non customers claiming deposit into accounts in response to offers for job, awards, gift, lottery, inheritance etc.

6.11 Cash intensive businesses:

The risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewelers should also be categorized by banks as 'high risk' requiring enhanced due diligence. Banks are also required to subject these 'high risk accounts 'to intensified transaction monitoring. High risk associated with such accounts should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-IND.

6.12 Pre-Paid Payment Instruments

The RBI has issued first set of guidelines in 2009 under payment and settlement systems act 2007, for the regulation and issue of pre-paid payment instruments by the payment system operators (PSOs). As the Banks are authorised as PSOs, these guidelines become binding on them.

Pre-paid payment instruments are payment instruments that facilitate purchase of goods and services against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holder, by cash, by debit to a bank account, or by credit card.

The Pre-paid instruments can be issued as smart cards, Magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers and any such instruments which can be used to access the Pre-paid amount(collectively called payment Instruments hereafter).

The Pre-paid payment instruments that can be issued in the country are classified under the three categories viz.

(i) Closed system payment instruments; These are payment instruments issued by a person for facilitating the purchase of goods and services from him/it and do not permit cash withdrawal or redemption. As these systems do not facilitate payments and settlements for third party services, issue and operation of such instruments are not classified as payment systems.

(ii) Semi-closed system payment Instruments: These are redeemable at a group of clearly identified merchant locations/establishments which contract specifically with the issuer to accept the payment instrument. These instruments do not permit cash withdrawal or redemption by the holder.

(iii) Open system payment instruments: These can be used for purchase of goods and services at any card accepting merchant locations (point of sale terminals) and also permit cash withdrawal at ATMs.

The RBI guidelines on KYC/AML/CFT apply mutatis mutandi to all persons issuing pre-paid payment instruments. The use of pre-Paid payment instruments for cross border transactions shall not be permitted except for the payment instruments issued by authorised persons under FEMA guidelines.

The maximum value of any Pre-Paid payment instrument shall not exceed Rs.50,000.

6.13 NGO/NPO

Trusts, charities, NGOs and organizations receiving donations, other than NPOs/NGOs promoted by United Nations require higher levels of due diligence. As some of the NGOs are recipient of funds from foreign sources, RBI has advised Banks that while accepting foreign contribution to the credit of accounts of an association/organisation, it should be ensured that the concerned association/organisation is registered with MHA or has their prior permission to receive such foreign contribution and that no branch other than the designated branch accepts the foreign contribution.

7.0 Small Deposit Accounts

7.1 Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion.

Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together, the aggregate of all withdrawals and transfers in a month does not exceed rupees Ten Thousand (Rs 10,000.00) and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs1, 00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I, branches should open an account for him, subject to:

Any other evidence as to the identity and address of the customer to the satisfaction of the bank.

The provisions for opening of bank accounts with restrictions on total credits and outstanding balance, with introduction from an existing account holder or other evidence of identity and address to the satisfaction of the bank, were made to help persons who were not able to provide 'officially valid documents' for opening accounts. In view of provisions for 'Small Accounts' being included in the PML Rules, the extant

instructions for opening of 'Accounts with Introduction' as prescribed in our circular DBOD.No.AML.BC.28 /14.01.001/2005-06 dated August 23, 2005 and in paragraph 2.6 of the Master Circular stand withdrawn. Hence the introduction from another account holder who has been subjected to full KYC procedure mentioned earlier stands withdrawn.

7.2 While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

In terms of para 2.7 (B) (b) of the Master Circular, accounts opened only on the basis of NREGA Job Card are subject to limitation applicable to 'Small Accounts' as prescribed in our circular DBOD.AML.No.77/ 14.01.001/2010-11 dated January 27, 2011. This has caused inconvenience to customers, who are mostly from rural areas.

In modification of instructions quoted above, banks are advised that they may now accept NREGA Job Card as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'.

8.0 Monitoring of Transactions

8.1 Ongoing monitoring is an essential element of effective KYC procedures. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

8.2 Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract

the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Branches should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months.

9.0 Closure of accounts

Where the branch is unable to apply appropriate KYC measures due to non- furnishing of information and /or non-cooperation by the customer, the branch should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken only after getting the concurrence / consent of the Divisional Head.

10.0 Risk Management

10.1 With a view to comply with 100% KYC compliance, it has been decided to open all CASA accounts only at the Regional Processing Centre (RPC). The branch management is primarily responsible for proper customer due diligence and collection of documentary evidences for customer ID and address proof and verify with the original documents. Only after the satisfaction of KYC compliance it should be submitted to RPC. RPC is responsible for second checking and proper creation of Customer Master and capturing customer information.

10.2 Bank's internal audit / concurrent audit system has to play an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements.

10.3 As regards Term Deposits and other loans / advances accounts, the branch Management has to comply with KYC as per the extant guidelines issued by RBI from time to time.

10.4 Concurrent/ Internal Auditors should 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 should be put up before the Audit Committee of the Board on quarterly intervals.

10.5. Branches should classify the accounts of the customers at the time of opening based on whether it is Low, Medium or high risk in nature. Review of the risk categorization of the customer should be carried out at a periodicity of not less than once in 6 months.

11.0 Introduction of New Technologies – Credit cards/debit cards/ smart cards/gift cards

Branches should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking, mobile banking, etc. that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Branches are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of Internet / mobile banking and issuance of variety of Electronic cards that are being used by customers for buying goods and services, drawing cash from ATMs and electronic funds transfers and for add-on / supplementary cardholders also. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

12.0 Combating Financing of Terrorism (CFT)

12.1 In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Branches are, therefore, advised to ensure enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

12.2 As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. The updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc /committees/ 1267/ consolist.shtml. The list of terrorist individuals / entities updated by us is

made available under Frs.com> branch login>monitoring>RBI>terrorist list. Branches are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list.

Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Principal Officer Money Laundering so as to report to RBI and FIU-IND.

12.3 Branches are also advised to take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions viz. Iran, Uzbekistan, Pakistan, Turkmenistan and Sao Tome and Principe, as identified in FATF Statement.

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

i) 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.

ii) On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, banks should 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.

iii) 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 RBI would forward the designated lists to the banks requiring them to:

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 banks 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 should necessarily be conveyed on e-mail .

c) Banks shall also send by post a copy of the communication mentioned in (b) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, Centre-1, 4th Floor, Cuffe Parade, Colaba, Mumbai – 400005 and also by fax at No.022-22185792 The particulars apart from being sent by post/fax should necessarily be conveyed on e-mail .

d) Banks shall also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the state/UT where the account is held as the case may 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 banks 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 should necessarily be conveyed on e-mail.

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

iv) Freezing of financial assets

a)On receipt of the particulars as mentioned in paragraph iv(b) 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 banks are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services , reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

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 section51A 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) Branches shall freeze such accounts without prior notice to the designated individuals/entities.

v) 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 banks and the procedure as enumerated at paragraphs 2.13[(iii), (iv) and (v)] shall be followed.

e) Branches shall freeze such accounts without prior notice to the designated persons involved.

vi) 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 banks 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 (iv)(b) 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 may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

12.5 Jurisdictions that do not or insufficiently apply the FATF Recommendations

a) Banks are 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, banks should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks should 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) Banks should 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 should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

13.0 Correspondent Banking

13.1 Correspondent banking is the provision of banking services by one bank (the "Correspondent bank") to another bank (the "respondent bank") These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks have been advised by RBI to 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. Similarly, branches should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board.

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

13.2 Correspondent relationship with a "Shell Bank"

RBI has advised banks to refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Branches should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks.

Branches should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Branches should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

14.0 Wire Transfer

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

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

a) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

b) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

c) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.

d) 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.

14.2 Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets.

The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, branches must ensure that all wire transfers are accompanied by the following information:

(A) 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 may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

(B) Domestic wire transfers

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

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

14.3 Exemptions

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

14.4 Role of Ordering, Intermediary and Beneficiary banks

(a) Ordering Bank

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

(b) Intermediary bank

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

(c) Beneficiary bank

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

15.0 Principal Officer

15.1 Our bank has appointed General Manager (Inspection and Audit Department) as Principal Officer. The Principal Officer 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.

15.2 The Principal Officer will be also responsible for timely submission of CTR, STR and reporting of counterfeit notes to FIU-IND.

16.0 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)

16.1 Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies with regard to preservation and reporting of customer account information. Branches 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.

16.2 Maintenance of records of transactions

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

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

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

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

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

e) all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency.

16.3 Information to be preserved

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

a) The nature of the transactions;

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

c) The date on which the transaction was conducted and

d) The parties to the transaction

16.4 Maintenance and Preservation of record

a) Branches are required to maintain the records containing information in respect of transactions referred to in Rule 3 above. Branches should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, branches should maintain for at least ten years from the date of cessation of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

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

c) In paragraph 8.0 of this policy, branches have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other

relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

16.5 Reporting to Financial Intelligence Unit - India

a) In terms of the PMLA rules, banks are required to report information relating to cash and suspicious transactions 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,
New Delhi-110021.
Website - http://fiuindia.gov.in/

b) FIU-IND have placed on their website editable electronic utilities to enable the bank to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base.

c) In terms of instructions contained in paragraph 4.2 of this policy, branches are required to prepare a profile for each customer based on risk categorization. Further, vide paragraph 8.0, the need for periodical review of risk categorization has been emphasized. It is against this background our bank has acquired a software solution viz. 'AMLOCK' from M/s. 3i Infotech to facilitate Transaction Monitoring Mechanism 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.

17.0 Reporting Obligations under PMLA 2002 - Cash and Suspicious Transaction Reports

17.1 Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the banks have been advised to scrupulously adhere to the following:

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis (not on fortnightly basis) and the bank should 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 should be reported by the Principal Officer to FIU-IND immediately in the specified format (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may 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 should 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 should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

vi) In case of Cash Transaction Reports (CTR) compiled centrally by the bank for the branches having Core Banking Solution (CBS) at their central data centre level, the bank may 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 generated in the format prescribed by Reserve Bank as per Master Circular on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002;

b) Large value transactions of individual branches are made available as part of the Exceptional Reports. All the branches have to study the report and report suspicious transactions, if any to Principal Officer, Money Laundering.

vii) For Integrally connected cash transactions referred to at 16.2 (b), the following clarification is given:

For example, from the following transactions taken place in a branch during the month of April 2008, for the purpose of reporting under integrally connected cash transactions, only the debit transactions are taken because total cash debits during the calendar month exceeds Rs10 lakhs. However, the bank should report only the debit transaction taken place on 02 /04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the bank, which is less than Rs 50,000/-.

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	

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 should not be reported by branches.

17.2 Suspicious Transaction Reports (STR)

i) While determining suspicious transactions, branches should 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 should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

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

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, branches are advised to refer to the indicative list of suspicious activities given in Annexure - II.

vi) Branches should not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no tipping off to the customer at any level. Branches and employees' should keep the fact of furnishing of STR strictly confidential.

17.3 Non-Profit Organisation

The report of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

18.0 Customer Education / Employee's Training

18.1 Customer Education

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

18.2 Employee's Training

The bank must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should 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.

18.3 Hiring of Employees

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

19.0 Risk based Transaction monitoring under "KYC/AML"

- For this various risks like Customer Risk, product Risk, Service Risk, Geographic Risk and other variables that may impact risk such as purpose of account, level of asset, level of regulation, duration of relationship, familiarity with the country, and use of intermediate corporate vehicles or structures for routing transactions to be taken into account.

- Besides the generation of alerts at the centralized AML cell with the help of watch list (WL), Typology (TY), Transaction Monitoring (TM) and Risk Management System (RM), identification of suspicious transaction by branches/departments can also be mooted through Customer verification (CV). Law Enforcement Agency Query (LQ), Media Reports (MR), Employee Initiated (EI), Public Complaint (PC) and Business Associates (BA).

- Management of alerts to be done based on factors such as source of Alert, Alert Indicator, customer profile, Risk Rating, pattern of Transaction and any additional information. Alerts of high risk customers and high risk scenario need to be prioritized. The alerts that are in tune with the profile of the customer and not appearing suspicious to be closed as false positive and those which do not appear tune with the profie and fit in the normal transaction pattern to be flagged as filed and reported.

- ☞ The effectiveness of STR detection to be improved and reviewed through White Listing (Alerts of bonafide transactions and established/genuine customer). Fine tuning alert generation software, compliance arrangement, employees screening, employees training and audit process.

INDICATIVE LIST OF CUSTOMERS FALLING UNDER LOW, MEDIUM & HIGH RISK CATEGORY AS PER IBA WORKING GROUP

Low Risk Customer

1. People belonging to lower economic strata of the society whose accounts show small balances and low turnover [small deposit accounts as per RBI norms eg. Kalpatharu a/c-Product 169 in our Bank)

2. Salaried class employees whose salary structures are well defined (limited operations with their Salary and other beneficial Perks),

3. Government Department and Government owned companies

4. Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken [this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment]

5. Customers with a long-term and active business relationship with the bank.

Medium Risk Customer

1. Non Bank Financial Institution

2. Stock Brokerage
3. Import/Export

4. Gas Station

5. Car/Boat/Plane Dealership

6. Electronics

7. Travel Agency

8. Used Car Sales

9. Telemarketers

10. Providers of Internet café, Telecommunication Linked services

11. Dot com Company or Internet Providers

12. Pawn shops

13. Auctioneers

14. Cash Intensive business such as Restaurants, retail shops, parking garages, Fast food centre, movie theatres 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. Individual and entities listed in schedule to the order under section 51 A of the Unlawful Activities (Prevention) act, 1967 relating to the purposes of prevention of and for coping with terrorist activities. Individuals and entities in various UNSCR list such as UN 1267 etc.

2. Individuals and entities in watch list of Interpol and other similar International Organization

3. Customers with dubious reputation as per public information available or Commercially available watch lists

4. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high risk.

5. 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.

6. Customers based in high risk countries / jurisdictions or locations.

7. Politically exposed persons (PEP) of foreign origin and customers who are close relatives of PEP's and accounts of which PEP is the ultimate beneficial owner.

8. Non resident customers and foreign Nationals

9. Embassies and/or consulates, offshore (foreign) corporations/business

10. Non face to face Customers.

11. High Net worth Individuals (HNI)

12. Firms with 'sleeping partners'

13. Companies with close family share holding or beneficial ownership

14. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries where there is no legitimate commercial rationale.

15. 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.

16. Investment Management/Money Management Company/Personal Investment Company.

17. Accounts for" gate keepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.

18. Client accounts managed by professional service providers such as law firms, accountants, agents,brokers,fund managers, trustees, custodians etc,

19. Trusts. Charities, NGOs / NPOs [especially operating on a "cross-border" basis], unregulated clubs and organization that are run by receiving donations. [Excluding NPO's/NGO are promoted by United Nations or its agencies.

20. Money service business: including seller of: Money orders/Travelers' check/Money transmission/cheques cashing/currency dealing of exchange.

21. Business accepting third party cheques [except super markets or retail stores that accept payroll cheques/cash payroll cheques].

22. Gambling/gaming including "Junket Operators" arranging gambling tours.

23. Dealers in high value or precious goods[e.g. jewel, gems and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers].

24. Customers engaged in a business which is associated with higher levels of corruption [e.g. arms manufacturers, dealers and intermediaries].

25. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
26. Customers that may appear to be Multi level marketing companies etc.[e.g. the recent speak Asia accounts]

INDICATIVE LIST UNDER HIGH AND-MEDIUM RISKS PRODUCTS & SERVICES

1. Electronic funds payment services such as Electronic Cash (stored value and payroll cards) and Funds transfers.

2. Electronic Banking –Net Banking, RTGS payments

3. Private Banking both domestic and international

4. Trust and asset Management services

5. Monetary instruments such as Travelers' cheque

6. Foreign correspondent accounts

7. Trade finance (such as letters of credit)

8. Special use or concentration accounts

9. Lending activities, particularly loans secured by cash collateral and marketable Securities. Ex: Private finance, Gold loan lending, private lending to SHG.

10. Non deposit account services such as Non-deposit investment products and Insurance

11 Transactions undertaken for non-account holders [occasional and walk in customers] E.g. Issue of DD/PO for less than Rs.50, 000/- by way of accepting Cash regularly for Such non-customers

12 Provision of safe custody or safe deposit boxes

13. Currency Exchange Transaction

14. Project financing of sensitive industries in high–risk jurisdictions

15. Trade finance services and transactions involving high- risk jurisdictions

16. Services involving bank note and precious metal trading and delivery
17. Services offering anonymity or involving third parties.

18. Services offering Cash, monetary or bearer instruments: cross border transaction. Eg Pazee International, Tirupur Benefit

INDICATIVE LIST UNDER HIGH AND -MEDIUM RISK GEOGRAPHICS

A. COUNTRIES/JURISDICTIONS

1. Countries subject to sanctions embargoes or similar measures in UN Security Council Resolutions (UNSCR).

2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing risks. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies.

3 Tax havens or countries that are known for highly secretive banking and corporate law Practices.

4. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures

5. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.

6. Countries identified by credible sources as having significant levels of criminal activity.

7. Countries identified by the Bank as high-risk because of its previous experience, transaction history or other factors such as legal considerations or allegations of official corruption .

B. LOCATIONS

1. Locations within the country know as high risk for terrorist incidents or terrorist financing activities [e.g. sensitive cities/locations and affected districts like Kashmir, Assam]

2. Locations identified by credible sources as having significant level of criminals, terrorist, terrorist financing activity [Eg Nepal, border area of East India]

3. Locations identified by the Bank as high risk because of its prior experiences, transaction history or other factors [Eg: Pakistan].

Annexure – I

Customer Identification Procedure
Features to be verified and documents that may be obtained from Customers

Features	Documents
Accounts of Individuals - Legal name and any other names used	(i) Passport (ii) PAN card (III) Voter's Identity Card (iv) driving License (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of Bank(vii)Job cards issued by NREGA duly signed by an officer of the state government (viii) The letter issued by the unique identification Authority of India containing details of name, address and Aadhar number or any other document as notified by the central government in consultation with Reserve Bank of India or any other documents as may be required by the banking companies or financial institution or intermediatery.
- **Correct permanent address**	(i) Telephone Bill (ii) Bank account Statement (iii) letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) letter from employer (subject to satisfaction of the bank) (vii) A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address. (any one document which provides customer information to the satisfaction of the bank will suffice)
Accounts of Companies - Name of the company - Principal place of Business - Mailing address of the company - Telephone / FAX number	(i) Certificate of incorporation and memorandum & Article of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers and employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) copy of the telephone bill

Accounts of Partnership firms - Legal name - Address - Name of all partners and their addresses - Telephone number of the firm and partners.	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or employee of the firm to transact business on its behalf (iv) Any official valid document identifying the partners and the persons holding the Power of attorney and their addresses (v) Telephone bill in the name of the firm / partners.
Accounts of Trusts & Foundations - Name of trustees, Settlers, beneficiaries and signatories - Name and addresses of the founder, the managers / directors and the beneficiaries - Telephone / FAX number	(i) certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid documents to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their address (iv) resolution of the managing body of the foundation/ association (v) Telephone Bill
Accounts of Proprietorship concerns Proof of the name , address and activity of the concern	♦ Registration certificate (in the case of a registered concern) ♦ Certificate / license 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. ♦ License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India , Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities . ♦ Registration / licensing document issued by the Central Government or State Government Authority / Department ♦ Importer Exporter Code (IEC) issued by the office of Directorate General of Foreign Trade (DGFT) etc. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Annexure - II

An Indicative List of Suspicious Activities

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 traveller'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.

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.

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.

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.

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.

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.

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.

Certain Bank Employees arousing Suspicion

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

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

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans
- Large deposits immediately followed by wire transfers
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts
- Multiple deposits of money orders, Banker's cheques, drafts of third parties
- Transactions inconsistent with the purpose of the account
- Maintaining a low or overdrawn balance with high activity
- U type transactions.
- Washing of funds through accounts after leaving minimum balance before and after the transactions.
- Money mule transactions.

Check list for preventing money-laundering activities:

- 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).

- 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.

- A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

- A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

- A customer experiences increased wire activity when previously there has been no regular wire activity.

- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

- A business customer uses or evidences or sudden increase in wired transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.

- 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.

- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions

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

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

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

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

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

• 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

• 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

o The amount is very large (say over Rs.10 lakhs)
o The amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any)
o The funds come from a foreign country or
o Such transactions occur repeatedly.

• A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques Oust under a specified threshold)

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

****