भारतीय रिजर्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/ 2011-12/79

UBD.BPD.(PCB).MC.No. 16 /12.05.001/2011-2012 July 1, 2011

Chief Executive Officers of
All Primary (Urban) Co-operative Banks

Dear Sir

Master Circular on Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, 2002

Please refer to our Master Circular UBD.BPD. (PCB).MC.No.16 /12.05.001/2010-11 dated July 1, 2010 on the captioned subject (available at RBI website www.rbi.org.in). The enclosed Master Circular consolidates and updates all the instructions / guidelines issued on the subject up to June 30, 2011 and mentioned in the appendix.

Yours faithfully

(Uma Shankar)
Chief General Manager

शहरी बैंक विभाग, केन्द्रीय कार्यालय, गारमेंट हाउस, पहली मंजिल, वरली, मुंबई - 400 018
फोन: 022 - 2493 9930 - 49, फैक्स: 022 - 2497 4030 / 2492 0231, ई मेल: cgmincubd@rbi.org.in

Urban Banks Department, Central Office, 1 Floor, Garment House, Worli, Mumbai - 400 018
Phone: 022 - 2493 9930 - 49, Fax: 022 - 2497 4030 / 2492 0231, Email: cgmincubd@rbi.org.in

Structure

Paragraph No.	Particulars	Page No.
1	Introduction	1
1.1	KYC /AML/CFT	1
1.2	Definition of customer	1
2	Guidelines	2
2.1	General	2
2.2	KYC Policy	2
2.3	Customer Acceptance Policy	2
2.4	Customer Identification Procedure	4
2.5	Customer Identification Requirements – Indicative Guidelines	6
2.6	Small deposit accounts	8
2.7	Monitoring of transactions	9
2.8	Closure of accounts	10
2.9	Risk Management	10
2.10	Introduction of new technology – credit/debit/smart/gift card	11
2.11	Combating Financing of Terrorism	11
.12	Correspondent Banking	15
2.13	Wire Transfers	16
2.14	Principal Officer	19
2.15	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)	19
2.16	Cash and Suspicious Transaction Report	22
2.17	Customer Education/Training of Employees/ Hiring of Employees	24
	Annex – I – Indicative List of documents required for opening of accounts	26
	Annex – II – List of reporting formats	27
	Appendix –List of circulars consolidated in the Master Circular	28

Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT) / Obligations of banks under Prevention of Money Laundering Act (PMLA), 2002

Introduction

1. The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks are advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures with the approval of the Board is formulated and put in place. The guidelines issued by RBI are under Section 35 A of B R Act, 1949 (AACS) and any contravention of or non- compliance with the same may attract penalties under the relevant provisions of the Act.

Definition of Customer

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

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Guidelines

2.1 General

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

ii) Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

iii) Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable, are strictly adhered to.

KYC Policy

2.2 Banks should frame their KYC policies incorporating the following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and
d) Risk Management.

2.3 Customer Acceptance Policy (CAP)

a) Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank

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

ii) Parameters of risk perception are clearly defined in terms of the nature of business activity , location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may

choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;

iii) 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;

iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/information furnished to the bank. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

v) 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 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 and

vi) 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 organisations etc.

b) Banks should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile banks 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.

c) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are

well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments 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 categorised 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. Banks 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 etc. However only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer.

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

Customer Identification Procedure (CIP)

2.4 (a) The policy approved by the Board of banks should clearly spell out 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. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need 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 bank 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 banks 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 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

b) 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, banks 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. Banks can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, banks 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.

c) Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.

d) An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in Annex-I to this Master Circular. It is clarified that permanent correct address, as referred to in Annex-I, 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.

e) It has been brought to our notice that the said indicative list furnished in Annex -I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

Customer Identification Requirements – Indicative Guidelines

2.5 (i) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks 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, banks should take reasonable precautions to verify the identity of the trustees and the settlors 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.

ii) Accounts of companies and firms

(a) Banks need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with banks. Banks 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.

(b) Certain firms posing as Multi Level Marketing (MLM) agencies for consumer goods and services have been mobilizing large deposits from the public (with promise of high return) by opening accounts at various bank branches. These funds running into crores of rupees, were being pooled at the principal accounts of the MLM Firms and were eventually flowing out of the accounts for purpose appearing illegal or higly risky. Accordingly, while opening agency accounts in the name of a proprietary concern the following documents need to be obtained and verified.

(i) Identity as also the address proof of the proprietor, such as passport, PAN card, Voter ID card, Driving Licence, Ration Card with photo, etc. – any one of the document is obtained.

(ii) Proof of the name, address and activity of the concern, like registration certificate(in the case of a registered concern)), certificate /licence issued by the Municipal authorities under Shop and Establishment act, sales and income tax returns, CST / VAT certificate, Licence issued by the registering authority like Certificate of Practice issued by the Institute of Chartered Accountants of India, Institute of Companies Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, any certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, etc. any two of the documents are to be obtained. These documents should be in the name of the proprietory concern.

iii) Client accounts opened by professional intermediaries

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks 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 banks 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 bank.

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

iv) 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. Banks 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. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks 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 and accounts where PEP is the ultimate beneficial owner. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, Banks should obtain senior management 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.

v) Accounts of non-face-to-face customers

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

vi) Opening of bank accounts – Salaried Employees

It has been brought to our notice that 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. It is, therefore, 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 licence, 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.

Small Deposit Accounts

2.6 (i) 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 and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) 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 of this master circular, banks should open an account for him, subject to:

Introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer,

or

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

ii) 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.

Further, banks were advised to open accounts with reduced KYC standards in respect of persons affected by floods to enable them to credit the grant received from the Government. These accounts shall also be treated at par with the accounts opened as per above instructions. However, the maximum balance in such accounts may be permitted as the amount of grant received from the Government or Rs. 50,000 whichever is more and the initial credit of the grant amount shall not be counted towards the total credit.

Monitoring of Transactions

2.7.1 Ongoing monitoring is an essential element of effective KYC procedures. Banks 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. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months. Banks are also required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorisation 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 transactions.

2.7.2 In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & Jewellers should also be categorised by banks as “high risk” requiring enhanced due diligence.

2.7.3 It is advised that high risk associated accounts should be taken

into account by banks to identify Suspicious Transactions Reports

Closure of accounts

2.8 Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

Risk Management

2.9 (a) The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers and apply various anti money laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.

b) Banks' internal audit and compliance functions have 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. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. 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.

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

2.10 Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are

required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks 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.

Combating Financing of Terrorism

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

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http:// www. un.org / sc/ committees / 1267 / consolist. shtml. Banks 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, banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

c) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51 A of the UAPA relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51 A, 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.

Banks are advised to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 and ensure meticulous compliance to the Order issued by the Government.

Banks are advised that on receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, they should ensure expeditious and effective implementation of the procedure prescribed under Section 51 A 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.

In terms of paragraph 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:

i. 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.

ii. 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 (MHA) 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.

iii. Banks shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, 4th Floor, Centre 1, Cuffe Parade, Colaba, Mumbai - 400 005 and also by FAX at No. 022-22185792. The particulars apart from being sent by post/FAX should necessarily be conveyed on e-mail.

iv. Banks shall also send a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the State/Union Territory where the account is held as the case may be and to FIU-IND.

v. 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), MHA at Fax No. 011 – 23092569 and also convey over telephone over 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

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

(d) Freezing of financial assets

i. On receipt of the particulars as mentioned in paragraph c (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the 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 five working days from the date of receipt of such particulars.

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

(iii) The Order shall take place without prior notice to the designated individuals/entities.

(e) Implementation of requests received from foreign countries under UNSCR 1373 of 2001

i. UNSCR 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 indirect by such persons and associated persons and entities.

ii. To give effect to the requests of foreign countries under UNSCR 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.

iii. 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 treats as designated individuals/entities.

iv. 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 2.11(c), (d) shall be followed.

v. The freezing orders shall take place without prior notice to the designated persons involved.

(f) 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 persons

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 bank concerned. 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 c (ii) above within two working days. The Joint Secretary, IS-I, MHA being the nodal officer for IS-I Division of MHA, shall cause such verification as 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 bank concerned. 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.

(g) Communication of Orders under Section 51A of Unlawful Activities (Prevention) Act, 1967

All Orders under Section 51 A of Unlawful Activities (Prevention) Act, 1967, relating to funds, financial assets or economic resources or related service, would be communicated to all banks through RBI. Banks are advised to

bring the provisions of the Unlawful Activities (Prevention) Act, 1967 to the notice of the staff concerned and ensure strict compliance.

(h) Deficiencies in AML / CFT regime in certain countries

Banks are also advised to take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions as identified in FATF Statement issued from time to time.

Correspondent Banking

2.12 (a) 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 should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, banks 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, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established 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.

b) Correspondent relationship with a "Shell Bank"

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

institutions that permit their accounts to be used by shell banks. Before establishing correspondent relationship with any foreign institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

Wire Transfer

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

i) 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.

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

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

(A) Cross-border wire transfers

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.

iii) Exemptions

Interbank transfers and settlements where both the originator and

beneficiary are banks or financial institutions would be exempted from the above requirements.

(iv) 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.

Principal Officer

2.14 (a) Banks should appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. With a view to enable the Principal Officer to discharge his responsibilities, it is advised that the

Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information. Further, banks should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors.

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

(c) The Principal Officer will also oversee and ensure overall compliance with regulatory guidelines on KYC / AML / CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended from time to time.

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)

2.15 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 in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 (as amended from time to time) 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.

(i) Maintenance of records of transactions

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

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

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

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

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

Explanation - Integrally connected cash transactions referred to at (b) above
The following transactions have taken place in a branch during the month of April , 2008:

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

As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakhs. However, the bank should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the bank, which is less than Rs.50, 000/-. 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 banks.

(ii) Information to be maintained

Banks are required to maintain the following information, including necessary information required for reconstruction of the transactions referred to in Rule 3:

a) the nature of the transactions;
b) the amount of the transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted; and
d) the parties to the transaction

(iii) Maintenance and Preservation of record

a) Banks are required to maintain the records (hard and soft copies)

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

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

c) In paragraph 2.7 of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof 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.

(iv) 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) Banks should carefully go through all the reporting formats. There are

altogether eight reporting formats, as detailed in Annex II, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR.

The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for banks to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.

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

d) In terms of instructions contained in paragraph 2.3(b) of this Master Circular, banks are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 2.7, the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

e) The CEOs of banks are advised to personally monitor the adherence by the bank officials to the provisions of the AML/ PMLA guidelines and ensure that sytems and procedures are put in place and instructions percolated to the operational levels. It should also be ensured that there is a proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

2.16 Cash and Suspicious Transaction Reports

Cash Transaction Report (CTR)

2.16.1 While detailed instructions for filing all types of reports are given in

the instructions part of the related formats, banks should 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 Principal Officer / controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule. In regard to CTR the cut off limit of Rs. 10 lakh is applicable to integrally connected cash transactions also.

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 banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised 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 in Para 2.15 (iv) (b) of this Master Circular.

b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this master circular at Para 2.15 (i), (ii) and (iii) respectively are

scrupulously followed by the branch. However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

Suspicious Transaction Reports (STR)

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

iii) Banks 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) As per extant instructions a bank should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. It is clarified that in the circumstances when a bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the bank should also file an STR with FIU-IND.

v)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.

vi) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, 2005'.

vii) Banks 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.

2.17 Customer Education/Employee's Training/Employee's Hiring
(a) Customer Education

Implementation of KYC procedures requires banks 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 banks to prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

b) Employee's Training

Banks 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.

c) Hiring of Employees

It may be appreciated that 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.

Annex – I (Para 2.4, 2.6)

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

Features	Documents
Accounts of individuals o Legal name and any other names used o Correct permanent address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence(v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority(iv) Electricity bill (v) Ration card(vi) Letter from employer (subject to satisfaction of the bank)(any one document which provides customer information to the satisfaction of the bank will suffice)
Accounts of companies o Name of the company o Principal place of business o Mailing address of the company o Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms o Legal name o Address o Names of all partners and their addresses o Telephone numbers of the firm and partners	(i) Registration certificate, if registered(ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations o Names of trustees, settlers, beneficiaries and signatories o Names and addresses of the founder, the managers/directors and the beneficiaries o Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses(iv) Resolution of the managing body of the foundation/association(v) Telephone bill

Annex – II

(List of various reports and their formats)

1. Cash Transaction Report(CTR)
2. Summary of CTR
3. Electronic File Structure – CTR
4. Suspicious Transactions Report(STR)
5. Electronic File Structure – STR
6. Counterfeit Currency Report (CCR)
7. Summary of CCR
8. Electronic File Structure - CCR

APPENDIX

Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002

A. List of Circulars consolidated in the Master Circular

No	Circular No	Date	Subject
1	UBD. CO. BPD. (PCB). Cir. No.9 /14.01.062/2010-11	02.05.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) –Standards – Primary (Urban) Co-operative Banks
2	UBD. CO. BPD.(PCB). Cir. No. 8/14.01.062/2010-11	02.05.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) – Standards – Primary (Urban) Co-operative Banks
3	UBD. CO. BPD.(PCB). Cir. No. 7 /14.01.062/2010-11	17.03.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT)
4	UBD. CO. BPD. (PCB) Cir. No. 6/14.01.062/2010-11	17.03.2011	Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) – Standards
5	UBD. BPD(PCB). No. 37/12.05.001/2010-11	18.02.2011	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
6	UBD. CO. BPD. No. 35/12.05.001/2010-11	10.01.2011	Opening of bank accounts – Salaried employees
7	UBD. BPD. (PCB).No. 32 / 12.05.001/2010-11	28.12.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
8	UBD. BPD. (PCB). Cir. No. 17 / 14.01.062/2010-11	25.10.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism
9	UBD. BPD. (PCB). Cir. No.12 / 12.05.001/2010-11	15.09.2010	Prevention of Money Laundering (Maintenance of the Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of records of the identioty of the Clients of the Banking companies, Financial Institutions and Intermediaries) Second Amendment Rules, 2010 – Obligation of banks
10	UBD. BPD. (PCB) No. 11 /12.05.001/2010-11	25.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
11	UBD. BPD. (PCB) No. 10/12.05.001/2010-11	23.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
12	UBD. BPD. (PCB) No. 9 / 12.05.001/2010-11	23.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002
13	UBD. BPD. (PCB) Cir. No. 7 / 14.01.062/2010-11	12.08.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism

14	UBD.BPD(PCB) Cir.No. 71/12.05.001/2009-10	15.06.2010	Prevention of Money Laundering (Maintenance of the Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of records of the identioty of the Clients of the Banking companies, Financial Institutions and Intermediaries)Amendment Rules, 2010 – Obligation of banks / All India Financial Institutions
15	UBD.BPD. CO.53/14.01.062/2009-2010	01.04.2010	Know Your Customer (KYC) Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism
16	UBD. BPD.CO.NSB 1/38/1203.000/2009-10	23.12.2009	Know Your Customer (KYC) Guidelines – Accounts of Proprietory Concern
17	UBD.(PCB) CO. BPD.Cir.No.36/14.01.062/2009 -10	18.12.2009	Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
18	UBD.(PCB) CO. BPD.Cir.No. 35/14.01.062/2009-10	17.12.2009	Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
19	UBD.(PCB). CO. BPD.Cir. No.33 /14.01.062/2009-10	17.12.2009	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)
20	UBD.CO.BPD.PCB.Cir.No. 23/12.05.001/2009-10	16.11.2009	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act, 2002 – Urban Cooperative Banks
21	UBD.CO.BPD.PCB.Cir.No.21/12.05.001/2009-10	16.11.2009	Combating Financing of Terrorism – Unlawful Activities (Prevention) Act, 1967 – Obligation of Banks – Urban Cooperative Banks
22	UBD. BPD.CO./NSB1/11/12.03.000/2009-10	29.09.2009	Know Your Customer (KYC) Guidelines – Accounts of Proprietory Concern
23	UBD.CO. BPD.PCB.Cir.No. 9/12.05.001/2009-10	16.09.2009	Adherence to KYC/AML guidelines while opening and conduct of the accounts of Multi Level Marketing Firms
24	UBD. CO. BPD (PCB) No. 1/12.05.001/2008-09	02.07.2008	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder – UCBs
25	UBD.CO.BPD.(PCB). No. 32 /09.39.000/2007-08	25.02.2008	Know Your Customer (KYC) Norms / Ant-Money Laundering (AML) Standards / Combating of Financing of Terrorism
26	UBD. CO. BPD. (PCB) No. 45/12.05.001/2006-07	25.05.2007	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) Wire Transfers
27	UBD.BPD. Cir. No.38 /09.16.100/2005-06	21.03.2006	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder – UCBs
28	UBD.BPD.PCB.Cir.11 /09.161.00/2005-06	23.08.2005	Know Your Customer Guidelines – Anti-Money laundering Standards – UCBs
29	UBD.PCB.Cir.No.6 /09.161.00/2005-06 dated August 3, 2005	03.08.2005	Facilitating opening of bank accountsfor flood affected persons
30	UBD.PCB.Cir. 30/09.161.00/2004-05	15.12.2004	Know Your Customer (KYC) Guidelines – Anti-Money Laundering Standards – UCBs
31	UBD.BPD.PCB.Cir.02/09.161.0	09.07.2004	'Know Your Customer' Guidelines - Compliance

	0/2004-05		
32	UBD.BPD.PCB.Cir. 48/09.161.00/2003-04	29.05.2004	'Know Your Custmer' Guidelines – Compliance
33	UBD.No.BPD.PCB.Cir. 41/09.161.00/2003-04	26.03.2004	'Know Your Customer' Guidelines – Compliance
34	UBD.No.DS.PCB.Cir.17/13.01. 00/2002- 03	18.09.2002	Guidelines on 'Know Your Customer 'Norms and 'Cash Transactions'