CUTTACK CENTRAL CO-OP. BANK LTD.

H.O.: Nimchouri, Cuttack - 753 002

MASTER CIRCULAR

Know Your Customer (KYC) Norms/
Anti-Money Laundering (AML) Standards/
Combating Financing of Terrorism (CFT)/
Obligation of Banks and Financial Institutions Under PMLA, 2002

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2015 – 16/42
DBR.AML.BC.No.15/14.01.001/2015-16

July 1, 2015
Ashadha 10, 1937(saka)

The Chairpersons/Chief Executive Officers
All Scheduled Commercial Banks/ Regional Rural Banks / All India Financial Institutions/ Local Area Banks/ All Primary (Urban) Co-operative Banks /State and Central Co-operative Banks

Dear Sir/Madam

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

Please refer to our Master Circular DBOD.AML.BC.No.22/14.01.001/ 14 –15 dated July 01, 2014 consolidating the instructions/guidelines issued till June 30, 2014 on the captioned subject.

2. This Master Circular consolidates instructions on the above matters issued up to June 30, 2015.

Yours faithfully,

(Lily Vadera)
Chief General Manager

Index

Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligation of banks and financial institutions under Prevention of Money Laundering Act, (PMLA), 2002.

A. Purpose

Banks and financial institutions (FIs) have been advised to follow certain customer identification procedure for opening of accounts and monitor transactions of suspicious nature for the purpose of reporting the same to appropriate authority. These 'Know Your Customer' (KYC) 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 FATF and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS), with suggestions wherever considered necessary, have been issued. Banks/FIs have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of their Boards.

A list of circulars issued from time to time in this regard which are consolidated in this Master Circular is given in Annex – III

B. Application

(i) The instructions, contained in the Master Circular, are applicable to All India Financial Institutions, all Scheduled Commercial Banks (including RRBs), Local Area Banks,/ All Primary (Urban) Co-operative Banks /State and Central Co-operative Banks.

(ii) These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

1. Introduction

The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.

2. Definitions

2.1 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

2.2 Designated Director

"Designated Director" means a person designated by the reporting entity (bank, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes:-

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the Managing Partner if the reporting entity is a partnership firm,

(iii) the Proprietor if the reporting entity is a proprietorship concern,

(iv) the Managing Trustee if the reporting entity is a trust,

(v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity, if the reporting entity is an unincorporated association or a body of individuals, and

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act

2.3 "Officially valid document" (OVD)

OVD means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, or any other document as notified by the Central Government in consultation with the Regulator.

(i) Provided that where 'simplified measures' are applied for verifying the identity of the clients the following documents shall be deemed to be OVD:

a) identity card with applicant's Photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;

b) Letter issued by a gazetted officer, with a duly attested photograph of the person.

(ii) Provided further that where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :.

a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

b) Property or Municipal Tax receipt;

c) Bank account or Post Office savings bank account statement;

d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

e) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and

f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

2.4 Person

In terms of PML Act a 'person' includes:

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm,

(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and

(vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

2.5 Transaction

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

(i) opening of an account;

(ii)deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

(iii) the use of a safety deposit box or any other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in whole or in part of any contractual or other legal obligation; or

(vi) establishing or creating a legal person or legal arrangement.

3. KYC Policy

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

(i) Customer Acceptance Policy (CAP);

(ii) Customer Identification Procedures (CIP);

(iii) Monitoring of Transactions; and

(iv) Risk Management.

3.1. Customer Acceptance Policy (CAP)

Banks/FIs should develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the bank/FIs and including the following aspects of customer relationship in the bank/FIs.

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

(ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the bank/FIs in categorizing the customers into low, medium and high risk ones.

(iii) Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.

(iv) Not to open an account where the bank/FI is unable to apply appropriate customer due diligence measures, i.e., the bank/FI is unable to verify the identity and /or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The bank/FI may also consider closing an existing account under similar circumstances.

(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.

(vi) The bank/FI should have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

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

3.2. Customer Identification Procedure (CIP)

3.2.1 General

(a) Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs. Banks/FIs need to obtain sufficient information to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the banking relationship. The bank/FI 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 the banks/FIs and a burdensome regime for the customers.

(b) Banks/FIs should have a policy approved by their Boards which should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e.,

(i) while establishing a banking relationship;

(ii) while carrying out a financial transaction;

(iii) when the bank/FI has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

(iv) when banks sell third party products as agents;

(v) while selling banks' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000/-.

(vi) when carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.

(vii) when a bank/FI has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

(c) Banks/FIs may seek 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other 'optional' customer details/additional information, if required, may be obtained separately after the account is opened only with the explicit consent of the customer.

3.2.2 I. Customer Due Diligence requirements (CDD) while opening accounts

A. Accounts of individuals:

(i) For opening accounts of individuals, banks/FIs should obtain one certified copy of an 'officially valid document' (as mentioned at paragraph 2.3 above) containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required by the bank/FI.

(ii) E-KYC service of Unique Identification Authority of India (UIDAI) should also be accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is to be treated as an 'Officially Valid Document'. Under e-KYC, the UIDAI transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/business correspondents/business facilitators, which may be accepted as valid process for KYC verification. The individual user, however, has to authorize to UIDAI by explicit consent to release her/his identity/address through biometric authentication to the banks/business correspondents/business facilitator. If the prospective customer knows only his/her Aadhaar number, the bank has to print the prospective customer's

e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned above. If the prospective customer carries a copy of the e-Aadhaar downloaded from a place/source elsewhere, still the bank has to print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal or adopt e-KYC procedure as mentioned above or confirm the identity and address of the resident through the authentication service of UIDAI

(iii) Since introduction is not necessary for opening of accounts under PML Act and Rules or the Reserve Bank's extant instructions, banks/FIs should not insist on introduction for opening of bank accounts.

(iv) **Simplified Measures for Proof of Identity:**

If an individual customer does not have any of the OVDs (as mentioned at paragraph 2.3 (i) above) as proof of identity, then banks/FIs are allowed to adopt 'Simplified Measures' in respect of 'Low risk' customers, taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category customers, where simplified measures are applied, it would be sufficient to obtain a certified copy of any one of the documents referred to at proviso to paragraph 2.3 (i) above., which shall be deemed as an OVD for the purpose of proof of identity.

(v) **Simplified Measures for Proof of Address:**

The additional documents mentioned at 2.3(ii) above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

(vi) **Small Accounts**

If an individual customer does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at paragraph 2.3 above), then 'Small Accounts' may be opened for such an individual. A 'Small Account' means a savings account in which:

- the aggregate of all credits in a financial year does not exceed rupees one lakh;

- the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand and
- the balance at any point of time does not exceed rupees fifty thousand.

A 'small account' maybe opened on the basis of a self-attested photograph and affixation of signature or thumb print.

Such accounts may be opened and operated subject to the following conditions:

a) the designated officer of the bank, while opening the small account, certifies under his signature that the person opening the account has affixed her/his signature or thumb print, as the case may be, in her/his presence;

b) a small account shall be opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account and that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place;

c) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

d) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism activity or other high risk scenarios, the identity of the customer shall be established through the production of "officially valid documents" and

e) foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of "officially valid documents".

(vii) A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD submitted for proof of

identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

(viii) Similarly, a customer is required to submit only one OVD as proof of address (either current or permanent) for KYC purpose. In case the proof of address furnished by the customer is neither the local address nor the address where the customer is currently residing, the bank should take a declaration from the customer of her/his local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted by the customer for such address. This address, however, should be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of letter, cheque books, ATM cards; telephonic conversation; visits to the place; etc. In the event of any change in this address due to relocation or any other reason, customers should intimate the new address for correspondence to the bank within two weeks of such a change.

(ix) In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address is to be submitted to the bank/FI within a period of six months.

(x) In case of close relatives, e.g. husband, wife, son, daughter and parents, etc. who live with their wife, husband, father/mother, daughter and son, who do not have officially valid document for address verification, then, in such cases, banks/FIs should obtain OVD for proof of address and identity of the relative with whom the prospective customer is living together with a declaration from the relative that the said person (prospective customer) proposing to open an account is a relative and is staying with her/him.

(xi) Banks are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Banks are advised that KYC verification once done by one branch of the bank should be valid for transfer of the account within the bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customers should be allowed to transfer their accounts from one branch to another branch without restrictions, without insisting on fresh proof of address and/or identity and on the basis of a self-declaration from the

account holder about his/her current address. Further, if an existing KYC compliant customer of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or address.

(xii) Where a customer categorised as low risk expresses inability to complete the documentation requirements on account of any reason that the bank considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the bank may complete the verification of identity within a period of six months from the date of establishment of the relationship.

(xiii) For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, banks/FIs may rely on a third party subject to the conditions that-

1) the bank/FI immediately obtains necessary information of such client due diligence carried out by the third party;
2) the bank/FI takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
3) the bank/FI is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;
4) the third party is not based in a country or jurisdiction assessed as high risk and
5) the bank/FI is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

(xiv) **Accounts of non-face-to-face customers**

With the introduction of phone 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.

(xv) **Procedure to be followed in respect of foreign students**

Banks should follow the following procedure for foreign students studying in India:

1) Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
2) Banks should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
3) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
4) The account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.
5) Students with Pakistani and Bangladesh nationality will need prior approval of the Reserve Bank for opening the account.

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

1) Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/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 such 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 a PEP should be taken at a senior level which should be clearly spelt out in the bank's Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an on-going basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

2) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, banks should obtain senior management's approval to continue the business relationship and subject the account to the CDD measures as applicable to PEPs including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

3) Further, banks should have appropriate ongoing risk management systems 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.

B. Accounts of persons other than individuals:

(i) **Where the customer is a company**, one certified copy each of the following documents are required for customer identification:

(a) Certificate of incorporation;

(b) Memorandum and Articles of Association;

(c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf and

(d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

Banks/FIs need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks/FIs. Banks/FIs 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.

(ii) Where the customer is a **partnership firm**, one certified copy of the following documents is required for customer identification:

(a) registration certificate;

(b) partnership deed and

(c) an officially valid document in respect of the person holding an attorney to transact on its behalf.

(iii) Where the customer is a **trust**, one certified copy of the following documents is required for customer identification:

(a) registration certificate;

(b) trust deed and

(c) an officially valid document in respect of the person holding a power of attorney to transact on its behalf.

(iv) Where the customer is an **unincorporated association or a body of individuals**, one certified copy of the following documents is required for customer identification:

(a) resolution of the managing body of such association or body of individuals;

(b) power of attorney granted to transact on its behalf;

(c) an officially valid document in respect of the person holding an attorney to transact on its behalf and

(d) such information as may be required by the bank/FI to collectively establish the legal existence of such an association or body of individuals.

(v) **Proprietary concerns**:

(1) For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern are required to be submitted:

(a) Registration certificate

(b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

(c) Sales and income tax returns.

(d) CST/VAT certificate.

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(f) Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

(h) Utility bills such as electricity, water, and landline telephone bills.

(2) Though the default rule is that any two documents, mentioned above, should be provided as activity proof by a proprietary concern, in cases where the banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

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

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines

and have undergone the required KYC due diligence/verification prescribed by SEBI through a Custodian/Intermediary regulated by SEBI. Such eligible/registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank (as detailed in Annex II of the circular DBOD.AML.BC.No.103/14.01.001/2013-14 dated April 3, 2014) would be required. Category I FPIs are, however, not required to submit the undertaking that "upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank". For this purpose, banks/FIs may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the PML Rules.

(vii) **When the client accounts are 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, however, should not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the banks. 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 into 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 a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

A gist of documents that can be accepted as proof of identity and address for various categories is furnished in Annex I

C. Beneficial ownership

When a bank/FI identifies a customer for opening an account, it should identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

(a) Where the **client is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-

1. *"Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.*
2. *"Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.*

(b) Where the **client is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

(c) Where the **client is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

(d) Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(e) Where the **client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person

exercising ultimate effective control over the trust through a chain of control or ownership.

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

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, banks/FIs should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks/FIs should insist on 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. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

II. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards

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 the same being used for money laundering purposes. 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 should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. 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. It is desirable that agents are also subjected to due diligence and KYC measures.

III. Periodic updation of KYC

A. **CDD requirements for periodic updation:** Banks/FIs should carry out periodical updation of KYC information of every customer, which should include the following:

(i) KYC exercise should be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Such KYC exercise may include all measures for confirming the identity and address and other particulars of the customer that the bank/FI may consider reasonable and necessary based on the risk profile of the customer, taking into account whether and when client due diligence measures were last undertaken and the adequacy of data obtained.

(ii) Banks/FIs need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', in case there is no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks/FIs should not insist on physical presence of such low risk customer at the time of periodic updation. The time limits prescribed at (i) above would apply from the date of opening of the account/ last verification of KYC.

(iii) Fresh photographs to be obtained from minor customer on becoming major.

B. **Freezing and closure of accounts**

(i) In case of non-compliance of KYC requirements by the customers despite repeated reminders by banks/FIs, banks/FIs may impose 'partial freezing' on such KYC non-compliant accounts in a phased manner.

(ii) During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force.

(iii) While imposing 'partial freezing', banks/FIs have to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirements to be followed by a reminder giving a further period of three months.

(iv) Thereafter, banks/FIs may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts.

(v) If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks/FIs should disallow all debits and credits from/to the accounts thereby, rendering them inoperative.

(vi) Further, it would always be open to the bank/FI to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level.

In the circumstances when a bank/FI believes that it would no longer be satisfied about the true identity of the account holder, the bank/FI should file a Suspicious Transaction Report (STR) with Financial Intelligence Unit – India (FIU-IND) under Department of Revenue, Ministry of Finance, Government of India.

IV. Miscellaneous

A. At-par cheque facility availed by co-operative banks

Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangement, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, banks should retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

In this regard, Urban Cooperative Banks (UCBs) are advised to utilize the 'at par' cheque facility only for the following purposes:

(i) For their own use.

(ii) For their account holders who are KYC complaint provided that all transactions of Rs.50,000/- or more should be strictly by debit to the customer's account.

(iii) For walk-in customers against cash for less than Rs.50,000/- per individual.

In order to utilise the 'at par' cheque facility in the above manner, UCBs should maintain the following:

(i) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.

(ii) Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

UCBs should also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.

B. Operation of Bank Accounts & Money Mules

"Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules". In order to minimise the operations of such mule accounts, banks should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

C. Simplified norms for Self Help Groups (SHGs)

KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary

D. Walk-in Customer

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. If a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify the identity and address of the customer and also consider filing a Suspicious Transactions Report (STR) to Financial Intelligence Unit – India (FIU-IND).

In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

E. Issue of Demand Drafts, etc, for more than Rs.50,000/-

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 Rs.50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment.

Banks should not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

F. Unique Customer Identification Code

A Unique Customer Identification Code (UCIC) will help banks to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. Banks have been advised to allot UCIC while entering into new relationships with individual customers as also the existing customers.

3.3. Monitoring of Transactions

3.3.1 Ongoing monitoring

Ongoing monitoring is an essential element of effective KYC/AML procedures. Banks/FIs should exercise ongoing due diligence with respect to every customer and

closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

(a) The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

(b) Banks/FIs should pay particular attention to the following types of transactions:

(i) large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

(ii) transactions which exceed the thresholds prescribed for specific categories of accounts.

(iii) transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

(iv) high account turnover inconsistent with the size of the balance maintained.

(c) Banks/FIs 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.

(d) Banks should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Banks should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the bank and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

3.4. Risk Management

3.4.1 Banks/FIs should exercise on going due diligence with respect to the business relationship with every client and closely examine the transactions in

order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds.

The Board of Directors should ensure that an effective AML/CFT programme is in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters. In addition, the following may also be ensured for effectively implementing the AML/CFT requirements.

(i) Using a risk-based approach to address management and mitigation of various AML/CFT risks.

(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation by the compliance functions of bank/FI's policies and procedures, including legal and regulatory requirements.

(iv) Concurrent/internal audit to verify the compliance with KYC/AML policies and procedures.

(v) Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

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

(b) Banks/FIs should categorise their customers into low, medium and high risk category based on their assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The banks/FIs are advised to have clear Board approved policies for risk categorisation and ensure that the same are meticulously complied with to effectively help in combating money laundering activities. The nature and extent of due diligence, may be based on the following principles:

(i) Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, may be categorised as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc. Further, Non-Profit Organisations (NPOs)/ Non-Government Organisations (NGOs) promoted by the United Nations or its agencies, and such international/ multilateral organizations of repute, may also be classified as low risk customers.

(ii) Customers who are likely to pose a higher than average risk should be categorised as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, may, if considered necessary, be categorised as high risk.

The above guidelines for risk categorisation are indicative and banks/FIs may use their own judgement in arriving at the categorisation for each account based on their own assessment and risk perception of the customers and not merely based on any group or class they belong to. Banks may use for guidance in their own risk assessment, the reports and guidance notes on KYC/AML issued by the Indian Banks Association.

4. Correspondent Banking and Shell Bank

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 may take the following precautions while entering into a correspondent banking relationship:

(a) Gather sufficient information to fully understand the nature of business of the bank including information on 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 bank's home country.

(b) Such relationships may be established only with the approval of the Board, or by a Committee headed by the Chairman/CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.

(c) The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented.

(d) In 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.

(e) The correspondent bank should ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(f) Banks should be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(g) Banks should ensure that their respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

(h) Banks should not 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 not affiliated to any regulated financial group).

(i) The correspondent bank should not permit its accounts to be used by shell banks.

5. Wire Transfer

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

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

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

(ii) 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.

(iii) 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.

(iv) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

(b) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating the same. 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/FIs must ensure that all wire transfers are accompanied by the following information:

1. Cross-border wire transfers

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

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

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

2. Domestic wire transfers

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

(ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50,000/- (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 at (i) above should be included in the message.

(c) Exemptions

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

(d) Role of Ordering, Intermediary and Beneficiary banks

(i) Ordering Bank

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

(ii) Intermediary bank

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

(iii) Beneficiary bank

A beneficiary bank 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.

6. Maintenance of KYC documents and Preservation period

PML Act and Rules cast certain obligations on the banks/FIs in regard to maintenance, preservation and reporting of customer account information. Banks/FIs are, therefore, advised to go through the provisions of the PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of the Act and the Rules *ibid.*

6.1 Maintenance of records of transactions

Banks/FIs should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

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

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

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

(iv) 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

(v) All suspicious transactions, whether or not in cash, made as mentioned in the Rules.

Banks/FIs are required to maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

(i) the nature of the transactions;

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

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

6.2 Preservation of Records

Banks/FIs 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

(i) In terms of PML Amendment Act 2012, banks/FIs should maintain for at least five years from the date of transaction between the bank/FI and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

(ii) Banks/FIs should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules *ibid*. The identification of records and transaction data should be made available to the competent authorities upon request.

(iii) Banks/FIs may maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 in hard or soft format.

(iv) As mentioned in paragraph 3.3.1(i) of this Master Circular, banks/FIs are required 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 to scrutinize the transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

7. Combating Financing of Terrorism

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC).

(a) **The "Al-Qaida Sanctions List",** includes names of individuals and entities associated with the Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

(b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at http://www.un.org/sc/committees/ 1988/list.shtml.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Banks/FIs are required to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, discussed below. Banks/FIs should ensure that they do not have any account in the name of individuals/entities appearing in the above lists. Details of accounts resembling any of the individuals/entities in the list should be reported to FIU-IND.

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

(a) 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 (Annex II of this circular) detailing the

procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for 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.

(b) Banks/FIs are required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex II of this Master Circular) and ensure meticulous compliance to the Order issued by the Government.

7.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) Banks/FIs 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/FIs should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks/FIs 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/FIs 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.

8. Reporting Requirements

a) Reporting to Financial Intelligence Unit - India

(i) In terms of the Rule 3 of the PML (Maintenance of Records) Rules, 2005, banks/FIs are required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations (NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021
Website - http://fiuindia.gov.in/

(ii) FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website. Banks/FIs should carefully go through all the reporting formats prescribed by FIU-IND.

(iii) FIU-IND have placed on their website editable electronic utilities to file electronic Cash Transactions Report (CTR)/ Suspicious Transactions Report (STR) to enable banks/FIs which 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 those banks/FIs, where all the branches are not fully computerized, the Principal Officer of the bank/FI 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 on their website http://fiuindia.gov.in

(iv) In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Banks/FIs are advised to take note of the timeliness of the reporting requirements.

In terms of instructions contained in paragraph 3.4 (b) of this Master Circular, banks/FIs are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 3.2.2. (III), the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that, as a part of their transaction monitoring mechanism, banks/FIs 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 the customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

b) Reports to be furnished to FIU-IND

1. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks/FIs should scrupulously adhere to the following:

(i) The 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 and banks/FIs 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 of the bank to FIU-IND in the specified format(Counterfeit Currency Report – CCR), by 15th day of the next month. 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 reports 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-IND. In case of CTRs compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre, banks may generate centralised CTRs in respect of the branches under core banking solution at one point for onward transmission to FIU-IND, provided the CTR is to be generated in the format prescribed by FIU-IND;

(vi) A copy of the monthly CTR submitted to FIU-India in respect of the branches should be available at the branches for production to auditors/inspectors, when asked for; and

vii) The instruction on 'Maintenance of records of transactions'; and 'Preservation of records' as contained above in this Master Circular at Para 6.1 and 6.2 respectively should be scrupulously followed by the branches.

viii) 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.

2. Suspicious Transaction Reports (STR)

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

(iii) Banks/FIs should make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) The STR should be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer 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, banks may consider the indicative list of suspicious activities contained in 'IBA's Guidance Note for Banks, January 2012'.

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

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.

4. Cross-border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed with FIU-IND by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

9. General Guidelines

(i) **Confidentiality of customer information:**

Information collected from customers for the purpose of opening of account is to be treated as confidential and details thereof should not be divulged for the purpose of cross selling, etc. Information sought from the customer should be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer should be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It should be indicated clearly to the customer that providing such information is optional.

(ii) **Avoiding hardship to customers:**

While issuing operational instructions to branches, banks/FIs should keep in mind the spirit of the instructions issued by the Reserve Bank so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

(iii) **Sensitising customers:**

Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. Banks/FIs should, therefore, prepare specific literature/pamphlets, etc., to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.

(iv) **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/FIs as an integral part of their personnel recruitment/hiring process.

(v) **Employee training:**

Banks/FIs must have an ongoing employee training programme so that the members of staff are adequately trained in AML/CFT policy. The focus of the training should be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues should be ensured.

(vi) **Provisions of FCRA**

Banks should ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

(vii) **Applicability to overseas branches/subsidiaries**

The guidelines in this circular apply to the branches and majority owned subsidiaries located abroad, to the extent local laws in the host country permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of the Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

(viii) **Technology requirements:**

The AML software in use at banks/FIs needs to be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold/silver/platinum, payment of dues of credit cards/reloading of prepaid/travel cards, third party products, and transactions involving internal accounts of the bank.

(ix) **Designated Director**:

Banks/FIs may nominate a Director on their Boards as "designated Director", as required under provisions of the Prevention of Money Laundering (Maintenance

of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director may be communicated to the FIU-IND. UCBs/ State Cooperative Banks / Central Cooperative Banks can also designate a person who holds the position of senior management or equivalent as a 'Designated Director'. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.

(x) **Principal Officer:**

Banks/FIs may appoint a senior officer as Principal Officer (PO). The PO should be independent and report directly to the senior management or to the Board of Directors. The PO shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer may be communicated to the FIU-IND.