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.

Annex- I

Customer Identification Procedure

Documents that may be obtained from customers

Customers/Clients	Documents (Certified copy of any one of the following officially valid document)
Accounts of individuals - Proof of Identity and Address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v)Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number. Where 'simplified measures' are applied for verifying the identity of customers the following documents shall be deemed to be 'officially valid documents: i. 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; ii. letter issued by a gazetted officer, with a duly attested photograph of the person. Where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :. i. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill); ii. Property or Municipal Tax receipt;

	iii. Bank account or Post Office savings bank account statement; iv. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; v. 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 vi. Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.
Accounts of Companies	(a) Certificate of incorporation; (b) Memorandum and Articles of Association; (c) A resolution from the Board of Directors a power of attorney granted to its manage officers or employees to transact on behalf; and An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Partnership firms	(a) registration certificate; (b) partnership deed; and an officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Trusts	(a) registration certificate; (b) trust deed; and an officially valid document in respect of the

	person holding a power of attorney to transact on its behalf
Accounts of unincorporated association or a body of individuals	(a) resolution of the managing body of such association or body of individuals; (b) power of attorney granted to him 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 to collectively establish the legal existence of such an association or body of individuals.
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice • Registration certificate (in the case of a registered concern) • Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, • Sales and income tax returns • CST/VAT certificate • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities • Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. The complete Income Tax return(not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities. 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.

Annex II

File No.17015/10/2002-IS-VI
Government of India
Ministry of Home Affairs
Internal Security-I Division

New Delhi, dated 27th August, 2009

ORDER

Subject : Procedure for implementation of Section 51A of the Unlawful Activities (Prevention)Act, 1967

The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51A reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to –

(a) 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;

(b) 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;

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

The Unlawful Activities (Prevention) Act define "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

2. As regards appointment and communication of details of UAPA nodal officers -

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736(Tel), 011-23092569(Fax) and e-mail.

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc.

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies 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, stocks or insurance policies etc. with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies 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, stocks or insurance policies etc. held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall 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.

5. On receipt of the particulars referred to in paragraph 3(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, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act.

The order shall take place without prior notice to the designated individuals/entities.

Regarding financial assets or economic resources of the nature of immovable properties.

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity

along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours 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**

9. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail**.** MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.

The order shall take place without prior notice, to the designated individuals/entities.

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to 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. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit,

terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 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 Regulators. FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

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

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

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers.

18. The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers 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 4(ii) above within two working days.

19. 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 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. 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.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under Section 51A.

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the

individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

24. All concerned are requested to ensure strict compliance of this order.

(D .Diptivilasa)
Joint Secretary to Government of India

ANNEX –III

(List of Circulars on 'Know Your Customer' and monitoring of transactions consolidated in the Master Circular)

Sr. No.	Circular No. and date	Subject	Gist of instructions
1	DBOD.BP.BC.92/C.469-76 dated 12th August, 1976	Issue of DDs/TTs in excess of Rs.5,000/-	Applicants (whether customer or not) for DD/MT/TT/Travellers' cheques for amount exceeding Rs.10,000/- should affix Permanent Income Tax Number on the application.
2	DBOD.GC.BC.62/c.408(A)/87 dated 11th November, 1987	Frauds in banks-opening of new accounts.	Payment for imports should be made by debit to the accounts maintained with the same bank or any other bank and under no circumstances cash should be accepted for retirement of import bills. There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.
3	DBOD.BP.BC.114/C.469 (81)-91 dated 19th April, 1991	Misuse of banking channels for violation of fiscal laws and evasion of taxes – Issue and payment of demand drafts for Rs.50,000 and above.	Banks to issue traveilers' cheques, demand drafts, mail transfers, telegraphic transfers for Rs. 50,000/- and above by debit to customers' accounts or against cheques only and not against cash.
4	DBOD.BC.20/17.04.001/92 dated 25th August, 1992	Committee to enquire into various aspects relating to frauds and malpractices	Banks advised to adhere to the prescribed norms and safeguards while opening accounts etc.

Sr. No.	Circular No. and date	Subject	Gist of instructions
		in banks.	
5	DBOD.BP.BC.60/21.01.023/92 dated 21st December,1992	Diversion of working capital funds.	Banks to ensure that withdrawals from cash credit/overdraft accounts are strictly for the purpose for which the credit limits were sanctioned by them. There should be no diversion of working capital finance for acquisition of fixed assets, investments in associate companies/ subsidiaries and acquisition of shares, debentures, units of UTI and other mutual funds and other investments in the capital market.
6	DBOD.FMC.No. 153/27.01.003/93-94 dated 1st September, 1993	Monitoring of flow of funds.	Banks to be vigilant and ensure proper end use of bank funds/monitoring flow of funds. Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade/business requirements and cases of unusual trends. Doubtful cases to be reported to DBOD, Regional office.
7	DBOD.GC.BC.193/17.04.001/93 dated 18th November, 1993	Frauds in banks – Encashment of Interest/Dividend Warrants, Refund Orders etc.	Banks to be vigilant in opening new accounts without proper introduction, new accounts with fictitious names and addresses. Banks instructed to strictly adhere to the instructions issued on opening and operating of bank accounts.
8	DBOD.GC.BC.202/17.04.001/93 dated 6th December, 1993	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Customer identification while opening accounts including obtaining of photographs of customers while opening accounts.
9	DBOD.No.GC.BC.46/17.04.001 dated 22nd April, 1994	The Committee to enquire into various aspects relating to frauds	Clarifications given to banks regarding obtaining photographs of the depositors/account holder authorised to operate new

Sr. No.		Circular No. and date		Subject		Gist of instructions
				and malpractices in banks.		accounts with effect from 1.1.1994. Obtaining of photographs would apply to residents and non-residents and all categories of deposits including fixed/recurring/cumulative deposit accounts and also to those persons authorised to operate the accounts.
10		DBOD.BP.BC.106/21.01.001/94 dated 23rd September,1994		Fraudulent operations in deposit accounts-opening and collection of cheques/pay orders etc.		Banks to examine every request for opening joint accounts very carefully, look into the purpose, other relevant aspects relating to business, the financial position of the account holders and whether number of account holders are large. 'Generally crossed' cheques and payable to 'order' should be collected only on proper endorsement by the payee. Banks to exercise care in collection of cheques of large amounts and ensure that joint accounts are not used for benami transactions.
11		DBOD.BP.BC.57/21.01.001/95 dated 4th May, 1995		Frauds in banks – Monitoring of deposit accounts.		Banks to introduce system of close watch of new deposit accounts and monitoring of cash withdrawals and deposits for Rs.10 lakh and above in deposit, cash credit and overdraft accounts. Banks to keep record of details of these large cash transactions in a separate register.
12		DBOD.BP.BC.102/21.01.001/95 dated 20th September, 1995		Monitoring of Deposit Accounts.		Reporting of all cash deposits and withdrawals of Rs.10 lakhs and above with full details in fortnightly statements by bank branches to their controlling offices. Transactions of suspicious nature to be apprised to Head Office.

Sr. No.	Circular No. and date	Subject	Gist of instructions
			RBI to look into these statements at the time of inspections
13	DBOD.BP.BC.42/21.01.001/96 dated 6th April, 1996	Monitoring cash deposits and withdrawals of Rs.10 lakh and above in deposit/other accounts.	Banks asked to submit feedback on implementation of the system of close monitoring of large cash deposits and withdrawals of Rs.10 lakh and above.
14	DBOD.No.BP.BC.12/21.01.023/98 dated 11th February 1998	Furnishing of data-violation of secrecy obligations.	Banks should satisfy themselves that information sought will not violate the laws relating to secrecy in banking transactions except under compulsion of law, duty to the public to disclose, where interest of bank requires disclosure and where disclosure is made with the express or implied consent of the customer.
15	DBS.FGV.BC.56.23.04.001/98-99 dated 21st June, 1999	Report of the Study Group on Large Value Bank Frauds.	Banks advised to implement the main recommendations of the Study Group on Large Value Bank Frauds.
16	DBOD.COMP.BC.No.130/07.03.23/2000-01 dated 14th June, 2001	Internet Banking in India-Guidelines.	Banking facilities on Internet will be subject to the existing regulatory framework. Banks having physical presence in India only will be allowed to offer banking services over Internet to residents in India and any cross border transactions will be subject to existing exchange control regulations. Banks to establish identity and also make enquiries about integrity and reputation of the prospective customer. Internet accounts should be opened only after proper introduction and physical verification of the identity of the customer.
17	DBOD.BP.52/21.01.001/2001-02 dated 5th	Prevention of Terrorism Ordinance,2001-	Banks should keep a watchful eye on the transactions of the 23 terrorist organisations listed in the

Sr. No.	Circular No. and date	Subject	Gist of instructions
	December, 2001	Implementation thereof.	Schedule to the Ordinance. Violations of the extant Acts or normal banking operations must be reported to the appropriate authorities under the Ordinance under advice to RBI. Banks to undertake 'due diligence' in respect of the 'KYC' principle.
18	DBOD.AML.BC. 89/14.01.001/2001-02 dated 15th April, 2002	Freezing of funds pursuant to United Nations Security Council Resolution, 1390.	Accounts of individuals and entities listed should be immediately frozen as informed by the Security Council Sanctions Committee of the UN. If any transaction is detected involving any of these entities, banks to report to RBI promptly for necessary action.
19	DBOD.AML.BC. No.102/14.01.001/2001-02 dated 10th May,2002	Monitoring of accounts - compliance with instructions.	Banks should ensure that no new accounts are opened by banned organisations. Banks to strictly adhere to the extant guidelines regarding opening and monitoring of accounts. Banks to confirm having issued instructions for immediate compliance by the branches and controlling offices.
20	DBOD.AML.BC. 18/14.01.001/2002-03 dated August 16, 2002	Guidelines on "Know Your Customer" norms and "Cash transactions"	First circular on KYC. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer. The Board of Directors of the banks should have in place adequate policies that establish procedures to verify the *bona fide* identification of individual/ corporates opening an account. Branches of banks are required to report all cash deposits and withdrawals of Rs.10 lakhs and

Sr. No.	Circular No. and date	Subject	Gist of instructions
			above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices.
21	DBOD.NO.AML. BC.58/14.01.001 /2004-05 dated November 29, 2004	'Know Your Customer' (KYC)Guidelines – Anti Money Laundering Standards	Our guidelines were revisited to make those compliant with FATF recommendations and Basel Committee Report on CDD. Four pronged approach was prescribed to banks based on Customer Acceptance Policy, Customer Identification Procedure, Monitoring of Transaction and Risk Management.
22	DBOD.NO.AML. BC.28 /14.01.001/2005 -06 dated August 23, 2005	Know YourCustomer Guidelines- Anti-Money Laundering Standards	KYC guidelines on document requirement were relaxed for people belonging to financially disadvantageous sections in the society, who could open account with introductory reference.
23	DBOD.NO.AML. BC.63/14.01.001 /2005-06 dated February 15, 2006	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder	Reporting mechanism and formats were prescribed to banks to report cash and suspicious transactions to Financial Intelligence Unit- India (FIU-IND).
24	DBOD.AML.BC. No.77/ 14.01.001 / 2006-07 April 13, 2007	Wire transfers	Banks were advised to ensure that all wire transfers involving domestic and cross border fund transfers are accompanied by full originator information.
25	DBOD.AML.BC. No. 63/ 14.01.001/2007-08 dated February 18, 2008	Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)	Revised guidelines on KYC/AML issued on review of risk categorization of customers; periodical updation of customer identification data and screening mechanism for recruitment /hiring process of personnel.

Sr. No.	Circular No. and date	Subject	Gist of instructions
26	DBOD.AML.BC. No. 85/ 14.01.001/ 2007 -08 dated May 22, 2008	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder.	Revised guidelines issued on CTR and STR by banks to FIU-IND.
27	DBOD.AML.BC. No.12/14.01.001 /2008-09 dated July 1, 2008	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2008
28	DBOD.AML.BC. No.2/14.01.001/ 2009-10 dated July 1, 2009	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2009
29	DBS.CO.FrMC. No. 2605/23.04.001/ 2009-10 dated August 18, 2009	Adherence to KYC/AML Guidelines while opening & conducting accounts of MLM Companies	Banks were advised to exercise caution when opening accounts of marketing and trading firms and to monitor cases when large number of cheque books were issued to such companies and small deposits in cash were being made in a/cs.
30	DBOD.AML.BC. No.43/14.01.001 /2009-10 dated September 11, 2009	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	The Government amended the Prevention of Money Laundering Act, 2005 and it came into force with effect from June 01, 2009 as notified by the Government.
31	DBOD.AML.BC. No.44/14.01.001 /2009-10 dated September 17, 2009	Combating Financing of Terrorism- Unlawful Activities (Prevention) Act,(UAPA) 1967- Obligation of banks	Government of India, Ministry of Home Affairs issued an 'Order' dated August 27, 2009 detailing the procedure for implementation of Section 51A of UAPA
32	DBOD.AML.BC. No.68/14.01.001 /2009-10 dated	Prevention of Money laundering (Amendment)	Government of India Notification dated November 12, 2009 amended the Prevention of Money

Sr. No.	Circular No. and date	Subject	Gist of instructions
	January 12, 2009	Rules 2009- Obligation of banks /Financial Institutions	Laundering (Maintenance of records of the Intermediaries) Rules 2005
33	DBOD.AML.BC. No.80/14.01.001 /2009-10 dated March 26, 2010	Know Your Customer (KYC) guidelines- accounts of proprietary concerns	Customer identification procedure issued for account opening by proprietary concerns.
34	DBOD.AML.BC. No.95/14.01.001 /2009-10 dated April 23, 2010	Prevention of Money Laundering (Maintenance of records of the …Intermediaries) Amendment Rules, 2010 - Obligation of banks	Government of India Notification dated February 12, 2010 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
35	DBOD.AML.BC. No.108/14.01.00 1/2009-10 dated June 9, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Further clarifications issued to banks in regard to: suspicion of money laundering or terrorist financing; filing of STRs; PEPs and Principal Officer.
36	DBOD.AML.BC. No.109/14.01.00 1/2009-10 dated June 10, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Guidelines reiterated for Client accounts opened by professional intermediaries
37	DBOD.AML.BC. No.111/14.01.00 1/2009-10 dated June 15, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Banks advised to take into account risks arising from deficiencies in AML/CFT regime of the Jurisdictions included in FATF Statement and also publicly available information of countries which do not or insufficiently apply the FATF recommendations and banks should not enter into relationship with shell banks.
38	DBOD.AML.BC. No.113/14.01.00 1/2009-10 dated	Prevention of Money Laundering	Government of India Notification dated June 16, 2010 amended the Prevention of Money Laundering

Sr. No.	Circular No. and date	Subject	Gist of instructions
	June 29, 2010	(Maintenance of records of the …Intermediaries) Second Amendment Rules 2010	(Maintenance of records of the Intermediaries) Rules 2005
39	DBOD.AML.BC. No.38/14.01.001 /2010-11 dated August 31, 2010	Accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a proprietary concern
40	DBOD.AML.BC. No.50/14.01.001 /2010-11 dated October 26, 2010	Opening of bank accounts - salaried employees	Banks need to rely on 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. In addition to the certificate from employer, banks should insist on at least one of the officially valid documents as provided in the PML Rules.
41	DBOD.AML.BC. No.65/14.01.001 /2010-11 dated December 7, 2010	Operation of bank accounts & money mules	Banks advised that operations of money mules can be minimized if banks follow the guidelines contained in the Master Circular on KYC/AML/CFT/obligations of banks under PMLA, 2002
42	DBOD.AML.BC. No.70/14.01.001 /2010-11 dated December 30, 2010	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'.	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'. requiring enhanced due diligence and intensified transaction monitoring. High risk associated with such accounts should also be taken into account to identify suspicious transactions for filing suspicious transaction reports (STRs) to FIU-IND.
43	DBOD.AML.BC. No.77/14.01.001 /2010-11 dated January 27, 2011	Opening of "Small Account"	Government of India Notification dated December 16, 2011 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries)

Sr. No.	Circular No. and date	Subject	Gist of instructions
			Rules 2005 to include definition of 'Small Account' and the detailed procedure for opening 'small accounts'.
44	DBOD.AML.BC. No.36/14.01.001 /2011-12 dated September 28, 2011.	Know Your Customer Norms – Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number	Letter issued by the UIDAI is accepted as an officially valid document for opening all types of bank accounts
45	DBOD.AML BC.No.47/14.01. 001/2011-12 dated November 04, 2011	Payment of Cheques/Drafts/ Pay Orders/Banker's Cheques	With effect from April 1, 2012,cheques / Drafts/ Pay Orders/ Banker's cheques issued on or after April 1, 2012 are valid for three months from the date of issue.
46	DBOD. AML.BC. No.65 /14.01.001/2011 -12 dated December 19, 2011	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 (PMLA), 2002-Assessment and Monitoring of Risk	Banks may take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels. Banks should also have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach and adopt enhanced measures for products, services and customers with a medium or high risk rating.
47	DBOD AML BC No. 70 /14.01.001/2011	splitting of UNSC 1267 Committee's list	Banks may take into account both "Al-Qaida Sanctions List" and "1988 Sanctions List" for the

Sr. No.	Circular No. and date	Subject	Gist of instructions
	-12 dated December 30, 2011	of individuals and entities linked to Al-Qaida and Taliban	purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.
48	DBOD. AML.BC. No 93 /14.01.001/2011 -12 dated April 17, 2012	Know your Customer (KYC) guidelines - accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a sole proprietary concern
49	DBOD. AML.BC. No 109 /14.01.001/2011 -12 dated June 08, 2012	Know your Customer (KYC) guidelines- Unique Customer Identification Code for bank customers in India	Banks to introduce Unique Customer Identification system to track all facilities availed, monitor transactions in a holistic manner and to have better risk-profiling of customers. System should be in place by May 2013.
50.	DBOD. AML.BC. No 110 /14.01.001/2011 -12 dated June 08, 2012	Know your Customer (KYC) guidelines - Risk Categorization and updation of Customer Profile	Banks advised to complete the work of risk categorization and updation of risk profile of all customers by March 2013.
51	DBOD.AML.BC. No. 39/14.01.001/20 12-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should initiate submission of reports on the FINnet Gateway in TEST MODE from August 31, 2012 to test their ability to upload the report electronically.
52	DBOD.AML.BC. No. 49/14.01.001/20 12-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should 'go-live' from October 20, 2012 and banks may discontinue submission of reports in CD format and use only FINnet Gateway for uploading of reports in the new XML reporting format.
53	DBOD.AML.BC. No. 65/14.01.001/20 12-13 dated December 10, 2012	Know Your Customer (KYC) norms /Anti-Money Laundering (AML)	KYC norms were further simplified by issuing following instructions : (i) to have only one document for both identity and address if the address on the document submitted for identity proof is

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	same as that declared in the account opening form, (ii) introduction from an existing customer of the bank not mandatory when documents of identity and address are provided, (iii) If the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address, (iv) NREGA Job Card to be accepted as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'
54	DBOD.AML.BC. No.71/14.01.001 /2012-13 dated January 18, 2013	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 (PMLA), 2002	Procedure to identify beneficial owner as advised by Government has been specified.
55	DBOD.AML.BC. No. 78 /14.01.001/2012 -13 dated January 29, 2013	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of	To help a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a utility bill or other documents in their name as address proof immediately after relocating, banks were advised to transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Money Laundering Act (PMLA), 2002	declaration from the account holder about his/her current address, subject to submitting proof of address within a period of six months. Further, banks were also advised to accept rent agreement duly registered with State Government or similar registration authority indicating the address of the customer, in addition to other documents listed as proof of address in Annex I of our Master Circular on KYC/AML/CFT dated July 2, 2012.
56	RBI/2012-13/459 DBOD.AML.BC. No.87/14.01.001 /2012-13 dated March 28, 2013	Simplifying norms for Self Help Groups	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
57	DBOD. AML.BC. No.101 /14.01.001/2011 -12 dated May 31, 2013	Extending time period for allotting Unique Customer Identification Code (UCIC) for banks' customers in India	Considering the difficulties experienced in implementation the time for completing the process of allotting UCIC to existing customers was extended up to March 31, 2014.
58	DBOD.AML.BC. No.29 /14.01.001/2013 -14 dated July 12, 2013	To reiterate and strengthen certain existing guidelines on KYC/AML/CFT for strict compliance.	Investigations by the Reserve Bank in the light of alleged violation of KYC/AML guidelines by several banks have shown that these guidelines have been violated, particularly in the case of walk-in customers. The circular was issued to reiterate and strengthen certain existing

Sr. No.	Circular No. and date	Subject	Gist of instructions
			guidelines on KYC/AML/CFT for strict compliance.
59	DBOD.AML.BC. No. 34/14.01.001/2013-14 dated July 23, 2013	Simplifying norms for Periodical Updation of KYC	The issue was reviewed in the light of practical difficulties/constraints expressed by bankers/customers in obtaining/submitting fresh KYC documents at frequent intervals as the relative documents submitted earlier specially by low-risk customers have remained unchanged in most of the accounts. Accordingly, based on the suggestions received, revised instructions were received.
60	DBOD.AML.BC. No.44/14.01.001/2013-14 dated September 2, 2013	e-KYC Service of UIDAI – Recognising on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid Document' under PML Rules	In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, e-KYC service UIDAI has launched its. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005
61	DBOD.AML.BC. No.45/14.01.001/2013-14 dated September 2, 2013	Foreign students studying in India – KYC procedure for opening of bank accounts	Considering the difficulties faced by foreign students arriving in India in complying with the Know Your Customer (KYC) norms while opening a bank account due to non-availability of any proof of local address, norms were relaxed by allowing a time of one month for furnishing the proof of local address.
62	DBOD. AML.BC. No. 50/14.01.001/2013-14 dated September 3, 2013	Circular regarding Information sought by banks from customers	Banks were advised to collect only 'mandatory' information required for KYC purpose while opening an account and Other 'optional' customer details/additional information, if

Sr. No.	Circular No. and date	Subject	Gist of instructions
			required may be obtained separately after the account is opened only with the explicit consent of the customer. Further, it was reiterated that banks should keep in mind that the information (both 'mandatory' – before opening the account as well as 'optional'- after opening the account with the explicit consent of the customer) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes
63	DBOD.AML.BC. No.63/14.01.001 /2013-14 October 29, 2013	Due diligence in correspondent banking relationship	Some commercial banks have arrangements with co-operative banks wherein 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 facilitating their remittances and payments. Since the 'at par' facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, 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.
64	DBOD.AML.BC. No.80/14.01.001 /2013-14 dated	Amendment to Section 13(2) of PML Act	Banks have been advised to nominate a Director on their Boards as "designated Director"

Sr. No.	Circular No. and date	Subject	Gist of instructions
	December 31, 2013		to ensure compliance with the obligations under Section 13(2) of the Prevention of Money Laundering (Amendment) Act, 2012.
65	DBOD.AML.BC. No. 100/14.01.001/2013-14 dated March 4, 2014	Recognising E-Aadhaar as an 'Officially Valid Document' under PML Rules	Banks have been advised to accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following: a) If the prospective customer knows only his/her Aadhaar number, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above. b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above; or confirm identity and address of the resident through simple authentication service of UIDAI.
66	DBOD. AML. No. 16415 /14.01.001/2013-14 dated March 28, 2014	Reporting of Cross Border Wire Transfer Report on FINnet Gateway	As per advice of FIU-IND a new reporting format for reporting of cross border wire transfers has been introduced. This was necessitated by amendments to Prevention of Money Laundering (PML) Rules, notified by the Government of India vide Notification No. 12 of 2013 dated August 27, 2013 and in terms of amended Rule 3, every reporting entity is required to maintain the

Sr. No.	Circular No. and date	Subject	Gist of instructions
			record of all transactions including the record of all cross border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India.
67	DBOD.AML.BC. No.103/14.01.001/2013-14 dated April 3, 2014	Harmonization of KYC norms for Foreign Portfolio Investors (FPIs)	KYC norms in case of FPIs for opening bank accounts were rationalised of along the lines of instructions issued by SEBI.
66	DBOD.AML.BC. No. 119/14.01.001/2013-14 dated June 9, 2014	Clarification on Proof of Address	Norms for furnishing proof of address have been relaxed to allow submitting only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. It was also advised that in case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation; (iii) visits; etc. In the event of change

Sr. No.	Circular No. and date	Subject	Gist of instructions
			in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.
67	DBOD. AML.BC. No.124 /14.01.001/2013 -14 dated June 26, 2014	Unique Customer Identification Code (UCIC) for banks' customers in India	In view the requests received, from banks for allowing more time to complete the exercise of allotting UCIC to existing customers, it was decided to extend the time for completing the process of allotting UCIC to existing customers up to December 31, 2014.
68	DBOD.AML.BC. No.26/14.01.001 /2014-15 dated July 17, 2014	Amendment to Prevention of Money-laundering (Maintenance of Records) Rules Notified in 2013	KYC/AML/CFT instructions issued to Reporting entities were revised in view of the amendment to PML Rules, notified on August 27, 2013.
69	DBOD.AML.BC. No. 39/14.01.001/20 14-15 dated September 4, 2014	KYC/AML/CFT Norms - Client Due Diligence measures	It was decided to dispense with the requirement of 'positive confirmation' while periodically updating Client Due Diligence measures. It was also advised that physical presence of the customers may, however, not be insisted upon at the time of such periodic updations
70	DBOD. AML. BC. No. 44/14.01.001/20 14-15 dated October 21, 2014	Clarifications on periodic updation of low risk customers, non-requirement of repeated KYC for the same customer to open new accounts and partial	Banks were advised not to seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', to obtain a self-certification by the customer in case of no change in status with respect to their identities and addresses. In case of change of address of such 'low

Sr. No.	Circular No. and date	Subject	Gist of instructions
		freezing of KYC non-compliant accounts	risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks may not insist on physical presence of such low risk customer at the time of periodic updation. 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 proof of address for the purpose. In cases of non-compliance of KYC requirements by the customers despite repeated reminders by banks, banks were allowed to impose 'partial freezing' on such KYC non-compliant in a phased manner, after giving due notice.
71	DBR.AML.BC.No.77/14.01.001/2014-15 dated March 13, 2015	Know your Customer (KYC) guidelines – in respect of accounts of proprietary concerns	With a view to ease the process of opening bank accounts of proprietary concerns while keeping the default rule for submitting any two documents as activity proof by a proprietary concern, it was allowed that 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

Sr. No.	Circular No. and date	Subject	Gist of instructions
			themselves that the business activity has been verified from the address of the proprietary concern. It was further clarified that the list of registering authorities indicated in the Master circular is only illustrative and includes license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute, as one of the documents to prove the activity of the proprietary concern.
72	DBR. AML. BC. No.104/ 14.01.001/ 2014-15 dated June 11, 2015	Amendment to Prevention of Money Laundering (Maintenance of Records) Rules, 2005 – additional documents for the limited purpose of 'proof of address'	Based on the amendments to PML Rules notified vide Government of India's Gazette Notification dated April 15, 2015, banks/financial institutions were advised about certain additional documents for the limited purpose of proof of address under 'simplified measures'.

A. List of Circulars consolidated in the Master Circular for UCBs

Sr. No.	Circular No.	Date	Subject
1.	UBD.BPD.Cir.No.25 / 14. 01.062/2014-15	08.04.2015	Anti Money Laundering(AML) /Combating of Financing of Terrorism (CFT-Standards-UCBs/StCBs/DCCBs
2.	DCBR.BPD.(PCB/RCB).Cir.No. 24 /14.01.062/2014 -15	01.04.2015	Know your Customer (KYC) guidelines - accounts of proprietary concerns
3.	DCBR.CO.BPD(RCB)Cir. No.9/ 14. 062/ 014-15	07.01.2015	Designed Director-Amendment to Section 13(2) of Prevention of Money Laundering Act (PMLA)2002
4.	DCBR.CO.BPD. (AD). Cir. No.1/ 14. 062/ 014-15	13.11.2014	Anti Money Laundering(AML)/ Combating of Financing of Terrorism (CFT-Standards-UCBs
5.	DCBR.CO.BPD. (PCB).No.1/14.0 1.062/2014-15	05.11.2014	Designed Director-Amendment to Section 13(2) of Prevention of Money Laundering Act (PMLA)
6	UBD.BPD.(PCB). Cir.No.23 / 14. 01.062/2014-15	22.10.2014	Know your Customer (KYC) Norms/ Anti Money Laundering(AML)/Combating of Financing of Terrorism (CFT) Guidelines
7	UBD.BPD. (PCB). Cir.No.22 / 14. 01.062/2014-15	22.10.2014	Know your Customer (KYC) Norms-Clarification on Proof of address
8	UBD.BPD.(PCB).Cir.No.16/ 14.01.062/2014-15	16.09.2014	Simplification of KYC Norms - Creating Public Awareness
9	UBD.BPD(PCB) .Cir.No.15/ 14.01.062/2014-15	16.09.2014	Client Due Diligence measures
10	UBD.BPD.(PCB).Cir.No.5/ 14.01.062/2014-15	05.08.2014	Amendment to Prevention of Money-laundering (Maintenance of Records) Rules 2013

11		UBD.BPD.(AD). Cir.No.1/14.062/ 2014-15		31.07.2014		Anti Money Laundering(AML)/ Combating of Financing of Terrorism (CFT)/Obligation of Banks
12		UBD.BPD.(PCB).Cir.No.2/ 14.01. 062/ 2014-15		02.07.2014		Unique Customer Identification Code (UCIC) for banks' customers in India
13		UBD.BPD.(PCB)Cir.No.69/14.01 .062/2013-14		10.06.2014		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 (PMLA), 2002 - Clarification on Proof of Address - Primary (Urban) Co-operative Banks
14		UBD.BPD.(PCB).Cir.No.9/14.01. 062/2013-14		26.05.2014		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 (PMLA), 2002 - Harmonization of KYC Norms for Foreign Portfolio Investors (FPIs) - Primary (Urban) Co-operative Banks
15		UBD.BPD.(PCB).Cir.No.54/14.0 1.062/2013-14		07.04.2014		Reporting of Cross Border Wire Transfer Report on FINnet Gateway - Primary (Urban) Co-operative Banks
16		UBD.BPD.(PCB).Cir.No.50/14.0 1.062/2013-14		06.03.2014		Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 - Recognising e-Aadhaar as an 'Officially Valid Document' under PML Rules - Primary (Urban) Co-operative Banks
17		UBD.BPD.(PCB).Cir.No.48/14.0 1.062/2013-14		18.02.2014		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 (PMLA), 2002 -Amendment to Section 13(2) - Primary (Urban) Co-operative Banks
18		UBD.BPD.(PCB).Cir.No.32/14.0 1.062/2013-14		22.10.2013		Know Your Customer (KYC) / Anti Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 - 'At par' Cheque Facility extended to Cooperative Banks by Scheduled Commercial Banks
19		UBD.BPD.(PCB).Cir.No.15/14.0 1.062/2013-14		17.09.2013		Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention ofMoney Laundering Act (PMLA), 2002 - e-KYC Service of UIDAI – Recognising on-line Aadhaar Authentication (Electronic Verification Process) to be accepted as an 'Officially Valid Document' under PML Rules - Primary (Urban) Co-operative Banks
20		UBD.BPD(AD). Cir.No.4/14.01.0 62/2013-14		10.09.2013		KYC Procedure for Opening of Bank Accounts - Foreign Students Studying in India - Primary (Urban) Co-operative Banks - Primary (Urban) Co-operative Banks
21		UBD.BPD.(PCB).Cir.No.11/14.0 1.062/2013-14		05.09.2013		Know Your Customer (KYC) / Anti Money Laundering (AML)Standards / Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 – Information Sought by Banks from Customers - Primary (Urban) Co-operative Banks
22		UBD.BPD.(PCB		31.07.2013		Know Your Customer (KYC) /

		).Cir.No.2/14.01.062/2013-14				Anti Money Laundering (AML) Standards /Combating Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002 - Simplifying Norms for Periodical Updation of KYC - Primary (Urban) Co-operative Banks
23		UBD.BPD(PCB) Cir.No.54/14.01.062/2012-13		06.06.2013		Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines - Unique Customer Identification Code(UCIC) for Banks' Customers in India - Primary (Urban) Co-operative Banks
24		UBD.BPD(PCB) Cir.No.46/14.01.062/2012-13		03.04.2013		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), 2002Simplifying Norms for Self Help Groups - Primary (Urban) Co-operative Banks
25		UBD.BPD(PCB) Cir.No.39/14.01.062/2012-13		07.03.2013		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 - Primary (Urban) Co-operative Banks
26		UBD.CO.PCB.Cir.No.37/14.01.062/2012-13		25.02.2013		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
27		UBD.BPD(PCB) Cir.No.34/14.01.062/2012-13		28.01.2013		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
28		UBD.BPD(PCB) Cir.No.28/14.01.062/2012-13		19.12.2012		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 (PMLA), 2002
29		UBD.BPD.(PCB).Cir.No.14/14.01.062/2012-13		09.10.2012		Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines - Unique Customer Identification Code(UCIC) for banks' customers in India - Primary (Urban) Co-operative Banks
30		UBD.BPD.(PCB).Cir.No.8/14.01.062/2012-13		13.09.2012		Know Your Customer (KYC) / Anti-Money Laundering (AML) /Combating of Financing of Terrorism (CFT) - Risk Categorization and Updation of Customer Profiles - Primary (Urban) Co-operative Banks
31		UBD.CO.BPD(PCB).No.34/12.05.001/2011-12		11.05.2012		Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concerns
32		UBD.CO.BPD.No.24/12.05.001/2011-12		05.03.2012		Know Your Customer (KYC) norms / Anti Money Laundering Standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002- Assessment and monitoring of risk
33		UBD.BPD.(PCB).Cir.No.20/14.01.062/2011-12		01.03.2012		Implementation of Section 51A of UAPA, 1967 - Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al Qaida and Taliban
34		UBD.CO.BPD.No.10/12.05.001/2011-12		09.11.2011		Prevention of Money Laundering Act, 2002 (PMLA) and Rules thereunder - Reporting of CTR, STR etc. to FIU-India- Reporting format under project FINnet

35		UBD.BPD.PCB. No. 8/12.05.001/2011-12		09.11.2011		Know Your Customer Norms - Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhar number
36		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
37		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
38		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)
39		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
40		UBD.BPD (PCB) No.38/ 12.05.001/2010-11		15.03.2011		Amendments to Prevention of Money Laundering Rules, 2005
41		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
42		UBD.CO.BPD.No.35/12.05.001/ 2010-11		10.01.2011		Opening of bank accounts - Salaried employees
43		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
44		UBD.BPD.(PCB		25.10.2010		Know Your Customer (KYC)

		).Cir.No.17/ 14.01.062/2010-11				Norms / Anti-Money Laundering Standards (AML) / Combating Financing of Terrorism
45		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 identity of the Clients of the Banking companies, Financial Institutions and Intermediaries) Second Amendment Rules, 2010 - Obligation of banks
46		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
47		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
48		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
49		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
50		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 identity of the Clients of the Banking companies, Financial Institutions and Intermediaries) Amendment Rules, 2010 - Obligation of banks / All India Financial Institutions
51		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
52		UBD. BPD. (PCB).Cir. No. 41/12.05.001/ 2009-10		03.02.2010		Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Amendment Rules, 2009 - Obligation of banks / Financial institutions
53		UBD.BPD.CO.NSB1/38/1203.000/ 2009-10		23.12.2009		Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concern
54		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)
55		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)
56		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)
57		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
58		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
59		UBD.BPD.CO./ NSB1/11/12.03. 000/ 2009-10		29.09.2009		Know Your Customer (KYC) Guidelines - Accounts of Proprietory Concern
60		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
61		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
62		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
63		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
64		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
65		UBD.BPD.PCB.Cir.11/09.161.00/ 2005-06		23.08.2005		Know Your Customer Guidelines - Anti-Money laundering Standards - UCBs
66		UBD.PCB.Cir.No.6/09.161.00/ 2005-06		03.08.2005		Facilitating opening of bank accountsfor flood affected persons
67		UBD.PCB.Cir. 30/09.161.00/2004-05		15.12.2004		Know Your Customer (KYC) Guidelines - Anti-Money Laundering Standards - UCBs
68		UBD.BPD.PCB.Cir.02/09.161.00/ 2004-05		09.07.2004		'Know Your Customer' Guidelines – Compliance
69		UBD.BPD.PCB.Cir.48/09.161.0		29.05.2004		'Know Your Custmer' Guidelines – Compliance

		0/ 2003-04				
70		UBD.No.BPD.PCB.Cir.41/ 09.161.00/ 2003-04		26.03.2004		'Know Your Customer' Guidelines – Compliance
71		UBD.No.DS.PCB.Cir.17/13.01.00/2002-03		18.09.2002		Guidelines on 'Know Your Customer 'Norms and 'Cash Transactions

List of Circulars consolidated in the Master Circular RPCD.RRB.RCB.AML.BC.No.02/07.51.018/2014-15 dated July 1, 2014 for DCCBs & StCBs

Sr. No.	Circular No.	Date	Subject
1	RPCD.RRB.RCB.AML.No.4424/07.51.018/2014-15	31.10.2014	KYC - Clarification on Proof of Address
2	RPCD.RRB.RCB.AML.BC.No.39/07.51.018/2014-15	31.10.2014	Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT) Guidelines - Clarifications on Periodic Updation of Low Risk Customers, Non-Requirement of Repeated KYC for the Same Customer to Open New Accounts and Partial Freezing of KYC Non-Compliant Accounts
3	RPCD.RRB.RCB.AML.No.2797/07.51.018/2014-15	09.09.2014	Simplification of KYC Norms - Creating Public Awareness
4	RPCD.RRB.RCB.AML.BC.No.31/07.51.018/2014-15	09.09.2014	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 (PMLA), 2002 - Client Due Diligence measures
5	RPCD.RRB.RCB.AML.BC.No.14/07.51.018/2014-15	21.7.2014	Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under PMLA, 2002 – Amendment to Prevention

						of Money-Laundering (Maintenance of Records) Rules 2013
6		RPCD.RRB.RCB.AML.BC.No.12/07.51.018/2014-15		03.07.2014		Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) Guidelines - Unique Customer Identification Code (UCIC) for Banks' Customers in India
7		RPCD.RRB.RCB.AML.BC.No. 112/07.51.018/2013-14		16.06.2014		Harmonization of KYC norms for Foreign Portfolio Investors (FPIs)
8		RPCD.RRB.RCB.AML.BC.No. 111/07.51.018/2013-14		12.06.2014		Clarification on Proof of address
9		RPCD.RRB.RCB.AML.BC.No. 97/07.51.018/2013-14		25.04.2014		Reporting of Cross Border Wire Transfer Report on FINnet Gateway
10		RPCD.RRB.RCB.AML.BC.No. 92/07.51.018/2013-14		13.03.2014		Recognising e- Aadhaar as an 'Officially Valid Document' under PML Rules
11		RPCD.RRB.RCB.AML.BC.No. 75/07.51.018/2013-14		09.01.2014		Amendment to Section 13(2) of PMLA 2002
12		RPCD.CO.RRB.RCB.BC.No. 48/07.51.010/2013-14		29.10.2013		'At par' cheque facility extended to Cooperative Banks / Regional Rural Banks by Scheduled Commercial Banks
13		RPCD.RRB.RCB.AML.BC.No. 37/07.51.018/2013-14		18.09.2013		Foreign students studying in India
14		RPCD.RRB.RCB.AML.BC.No. 31/07.51.018/2013-14		16.09.2013		Information sought by banks from customers
15		RPCD.RRB.RCB.AML.BC.No. 32/07.51.018/2013-14		10.09.2013		e-KYC Service of UIDAI - Recognising on-line Aadhaar authentication (electronic verification process) to be

						accepted as an 'Officially Valid Document' under PML Rules
16		RPCD.RRB.RCB.BC.No.84/07.51.018/2013-14		25.07.2013		Simplifying norms for periodical updation of KYC
17		RPCD.RCB.RRB.AML.BC.No.76/07.51.018/2012-13		04.06.2013		Unique Customer Identification Code (UCIC) for banks' customers in India
18		RPCD.RCB.RRB.AML.BC.No.71/07.51.018/2012-13		01.04.2013		Simplifying Norms for Self Help Groups
19		RPCD.RRB.RCB.BC.No.63/07.51.018/2012-13		30.01.2013		Shifting of bank accounts to another centre-address proof
20		RPCD.RRB.RCB.BC.No.59/07.51.018/2012-13		22.01.2013		Identification of beneficial owner
21		RPCD.CO.RRB.RCB.AML.No.6097/7.51.018/2012-13		13.12.2012		Simplification of KYC documents
22		RPCD.CO.RRB.RCB.AML.BC.No.36/03.05.33(E)/2012-13 [@1]		15.10.2012		Uploading of reports on FINnet Gateway
23		RPCD.CO.RRB.RCB.AML.BC.No.29/03.05.33(E)/2012-13		18.09.2012		Uploading of reports in 'Test Mode' on FINnet Gateway
24		RPCD.CO.RRB.RCB.AML.BC.No.82/03.05.33(E)/2011-12		11.06.2012		Unique Customer Identification Code for bank customers in India
25		RPCD.CO.RRB.RCB.AML.BC.No.81/07.40.00/2011-12		11.06.2012		Risk Categorisation and updation of Customer Profile
26		RPCD.CO.RRB.RCB.AML.BC.No.70/07.40.00/		18.04.2012		Accounts of proprietary concerns

		2011-12				
27		RPCD.CO.RCB.AML.BC.No.52/07.40.00/2011-12		04.01.2012		Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban
28		RPCD.CO.RRB.AML.BC.No.51/03.05.33(E)/2011-12		02.01.2012		Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban
29		RPCD.CO.RCB.AML.BC.No.50/07.40.00/2011-12		30.12.2011		Assessment and Monitoring of Risk
30		RPCD.CO.RRB.AML.BC.No.46/03.05.33(E)/2011-12		21.12.2011		Assessment and Monitoring of Risk
31		RPCD.CO.RRB.AML.BC.NO.31/03.05.33(E)/2011-12		16.11.2011		Payment of Cheques / Drafts / Pay Orders / Banker's Cheques
32		RPCD.CO.RCB.AML.BC.No.23/07.40.00/2011-12		17.10.2011		Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
33		RPCD.CO.RRB.AML.BC.No.21/03.05.33(E)/2011-12		13.10.2011		Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
34		RPCD.CO.RRB.AML.BC.No.15/03.05.33(E)/2011-12		08.08.2011		Opening of "Small Account"
35		RPCD.CO.RCB.AML.BC.No.63/07.40.00/2010-11		26.04.2011		Opening of "Small Account"
36		RPCD.CO.RCB.AML.BC.No.50/07.40.00/2010-11		02.02.2011		Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'.
37		RPCD.CO.RRB.AML.BC.No.46/03.05.33(E)/20		12.01.2011		Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks

		10-11				as ' high risk'.
38		RPCD.CO.RCB.AML.BC.No.39/07.40.00/2010-11		27.12.2010		Operation of bank accounts & money mules
39		RPCD.CO.RRB.AML.BC.No.40/03.05.33(E)/2010-11		24.12.2010		Operation of bank accounts & money mules
40		RPCD.CO.RCB.AML.BC.No.37/07.40.00/2010-11		10.12.2010		Opening of bank accounts - salaried employees
41		RPCD.CO.RRB.AML.BC.No.31/03.05.33(E)/2010-11		06.12.2010		Opening of bank accounts - salaried employees
42		RPCD.CO.RF.AML.BC.No.20/07.40.00/2010-11		13.09.2010		Accounts of proprietary concerns
43		RPCD.CO.RRB.AML.BC.No.19/03.05.33(E)/2010-11		09.09.2010		Accounts of proprietary concerns
44		RPCD.CO.RF.AML.BC.No.12/4007.40.00/2010-11		20.07.2010		Prevention of Money Laundering (Maintenance of records of the ... Intermediaries) Second Amendment Rules 2010
45		RPCD.CO.RRB.AML.BC.No.13/03.05.33(E)/2010-11		22.07.2010		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 (PMLA), 2002
46		RPCD.CO.RF.AML.BC.No.11/07.40.00/2010-11		20.07.2010		Obligation of banks under PMLA, 2002
47		RPCD.CO.RF.AML.BC.No.89/07.40.00/2009-10		25.06.2010		Client Accounts opened by professional intermediaries
48		RPCD.CORRB.AML.BC.No.87/		23.06.2010		Know Your Customer (KYC) Norms / Anti-Money Laundering

		03.05.33(E)/2009-10				(AML) Standards / Combating of Financing of Terrorism (CFT) / Obligation of Banks under Prevention of Money Laundering Act (PMLA), 2002
49		RPCD.CO.RF.AML.BC.No.88/07.40.00/2009-10		25.06.2010		Filing of STRs; PEPs and Principal Officer
50		RPCD.CO.RRB.AML.BC.No.86/03.05.33(E)/2009-10		21.06.2010		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 (PMLA), 2002
51		RPCD.CO.RF.AML.BC.No.84/07.40.00/2009-10		14.05.2010		Government of India Notification dated February 12, 2010 amending the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
52		RPCD.CO.RF.AML.BC.No.83/07.40.00/2009-10		12.05.2010		Customer identification procedure issued for account opening by proprietary concerns.
53		RPCD.CO.RRB.AML.No.67/03.05.33(E)/2009-10		09.04.2010		Know Your Customer (KYC) Guidelines - Accounts of Proprietary Concerns
54		RPCD.CO.RF.AML.BC.No.83/07.40.00/2009-10 @2		03.03.2010		Prevention of Money laundering (Amendment) Rules 2009- Obligation of banks / Financial Institutions
55		RPCD.CO.RRB.No.39/03.05.33(E)/2009-10		05.11.2009		Combating Financing of Terrorism - Unlawful Activities (Prevention) Act, 1967 - Obligation of Banks
56		RPCD.CO.RF.AML.BC. No.34/07.40.00/2009-10		29.10.2009		Combating Financing of Terrorism- Unlawful Activities (Prevention) Act,(UAPA) 1967- Obligation of banks
57		RPCD.CO.RF.AML. BC.No.28/07.40.00/2009-10		30.09.2009		KYC norms / AML standards / CFT / Obligation of banks under PMLA, 2002

58		RPCD.CO.RRB.BC.No.27/03.05.33(E)/2009-10		29.09.2009		Know Your Customer (KYC) Norms / Anti- Money Laundering (AML) Standards and Obligation of Regional Rural Banks (RRBS) Under PMLA, 2002
59		RPCD.CO.RCB.AML.BC.No.81/07.40.00/2007-08		25.06.2008		Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder.
60		RPCD.CO.RRB.No.BC.77/03.05.33(E)/2007-08		18.06.2008		Prevention of Money Laundering Act, 2002 - Obligation of Banks in terms of Rules Notified there under
61		RPCD.CO.RF.AML.BC.No.51/07.40.00/2007-08		28.02.2008		Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)
62		RPCD.CO.RRB.No.BC.50/03.05.33(E)/2007-08		27.02.2008		Know Your Customer (KYC) Norms / Anti- Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)-RRBs
63		RPCD.CO.RRB.AML.BC.No.98/03.05.28-A/2006-07		21.05.2007		Wire Transfers - Regional Rural Banks (RRBs)
64		RPCD.CO.RF.AML.BC.No.96/07.40.00/2006-07		18.05.2007		Wire transfers
65		RPCD.CO.RRB.AML.BC.68/03.05.33(E)/2005-06		09.03.2006		Prevention of Money Laundering Act, 2002 - Obligation of Regional Rural Banks in terms of Rules notified thereunder
66		RPCD.CO.RF.AML.BC.No.65/07.40.00/2005-06		03.03.2006		Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder
67		RPCD.No.RRB.BC.33/03.05.33(E)/2005-06		23.08.2005		Know Your Customer Guidelines - Anti-Money Laundering Standards
68		RPCD.RF.AML.BC.No.30/07.40.00/2005-06 [@3]		23.08.2005		Know Your Customer Guidelines - Anti-Money Laundering Standards
69		RPCD.AML.BC.		18.02.2005		Know Your Customer (KYC)

		No.80/07.40.00 /2004-05				guidelines - Anti Money Laundering Standards
70		RPCD.No.RRB. BC.81/03.05.33 (E)/2004-05		18.02.2005		Know Your Customer (KYC) guidelines - Anti Money Laundering Standards

--------*----------*----------*----------*----------