POLICY

ON

Know Your Customer (KYC) Norms

Anti-Money Laundering (AML) Standards

Combating of Financing of Terrorism CFT)

Obligation of Bank Under PMLA

Revised as on 23/05/2014

THE CATHOLIC SYRIAN BANK LTD

HEAD OFFICE

Compliance & PMLA CELL

PREFACE

This Revised KYC Policy book-let is a consolidation of the instructions on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002.

Reserve Bank of India [RBI] has advised the banks to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority.

These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT).

Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued.

These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005.

Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

The Policy has been placed on the bank's website: [www.csb.co.in]

CONTENTS

Introduction

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

1. 2 Definition of Customer
For the purpose of KYC policy, a 'Customer' is defined as:

a person or entity that maintains an account and/or has a business relationship with the bank.

one on whose behalf the account is maintained (i.e. the beneficial owner). [Ref: Government of India Notification dated February 12, 2010 - Rule 9, sub-rule (1A) of PMLA Rules - ' Beneficial Owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person] beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

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

2. Guidelines

2.1 General

1. Branches / offices should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Branches / offices should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account.
2. Branches / offices should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.
3. Branches / offices should ensure that the provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable are strictly adhered to.

2.2 KYC Policy

The KYC Policy of the Bank is framed incorporating the following four key elements:
Customer Acceptance Policy;
Customer Identification Procedures;
Monitoring of Transactions; and
Risk Management.

2.3 Customer Acceptance Policy (CAP)

a) As per RBI guidelines, the bank has developed a Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The CAP enumerates explicit guidelines on the following aspects of customer relationship in the bank.

i)No account is opened in anonymous or fictitious/ benami name. [Ref: Government of India Notification dated June 16, 2010 Rule 9, sub-rule (1C) - Banks should not allow the opening of or keep any anonymous account or accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified].

ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk. Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;

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

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

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

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

b) Banks should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc.

c) The nature and extent of **due diligence** will depend on the risk perceived by the bank. However, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

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

e) Bank should take steps to identify and assess their Money Laundering (ML) / Terrorist Financing (TF) risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels.

Characteristics of High Risk Customers

1. **Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.**
2. **Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.**
3. **Individuals and entities in watch lists issued by Interpol and other similar International organizations**
4. **Customers with dubious reputation as per public information available or commercially available watch lists**
5. **Individuals and entities specifically identified by regulators, FIU and other competent authorities as high risk**
6. **Customers conducting their business relationship or transactions in unusual circumstances such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.**
7. **Politically exposed persons(PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;**
8. **Non-resident customers and foreign nationals.**
9. **Embassies/Consulates**
10. **Off-shore (foreign) corporation/business**
11. **Non face-to-face customers**
12. **High net worth individuals**
13. **Firms with 'sleeping partners'**
14. **Companies having close family shareholding or beneficial ownership**
15. **Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale**
16. **Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.**
17. **Investment Management / Money Management Company /Personal Investment Company**
18. **Trusts, charities, NGOs/NPOs**
19. **Money Service Business: including seller of : Money Orders/ Travelers' Checks/ Money Transmission/ Check Cashing/ Currency Dealing or Exchange**
20. **Gambling/gaming including "Junket Operators" arranging gambling tours**
21. **Dealers in high value or precious goods(e.g. jewel, gem and precious metals dealers**
22. **Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.**
23. **Customers engaged in industries that might relate to nuclear proliferation activities or explosives**
24. **Customers that may appear to be Multilevel marketing companies etc.**

Characteristics of Medium Risk Customers

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

16. **Notaries**
17. **Secretarial Firms**
18. **Accountants**
19. **Venture capital companies**

Indicative list of High/ Medium risk products And Services

1.Electric funds payment services such as Electric cash, fund transfers etc
2. Electronic banking
3.private banking
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6.Foreign correspondent accounts
7. Trade finance
8. Special use or concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities 10.Project financing of sensitive industries in high risk jurisdictions
11. Services offering cash, monetary or bearer instruments; cross-border transactions etc.
12. Non-deposit account services such as Non-deposit investment products and insurance

Indicative list of High/ Medium Risk Geographies

1. **Countries subject to sanctions, embargoes or similar measures in the United Nations security Council Resolutions("UNSCR")**
2. **Jurisdictions identified in FATF public statement as having substantial money laundering(ML) and terrorist financing (TF) risks**
3. **Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies**
4. **Tax havens or countries that are known for highly secretive banking and corporate law**
5. **Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.**
6. **Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.**
7. **Countries identified by credible sources as having significant levels of criminal activity**
8. **Countries identified by the bank as having high risk because of its prior experiences transaction history, or other factors**

Locations

1. **Locations within the country known as high risk for terrorist incidents or terrorist financing activities**
2. **Locations identified by credible sources as having significant levels of criminal ,terrorist, terrorist financing activity**
3. **Locations identified by the bank as high- risk because of its prior experiences, transaction history, or other factors.**

To enhance the level of managing and mitigating risk, HO-PMLA Cell should verify transactions of the following nature;

(a) Cash deposit of Rs.50,000 and above without PAN/Form 60/61
(b) Disbursal of Gold loan products of Rs.2 Lakh and above
(c) Any cash remittance to NRE accounts
(d) Structuring of transactions in accounts
(e) Random verification of transactions in high risk rated accounts
(f) Verification of genuineness of PAN with CBDT at branch level
(g) Monitoring of KYC compliance level in branches
(h) Monitoring of Periodical Updation of Customer Identification data and review of Risk Categorization
(i) Monitoring of large value cash transactions send through RTGS/NEFT

Low Risk Customers

Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met.

Medium Risk Customers

Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading / business activity.

Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

Customers that are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

High Risk Customers
The branches may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

Examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; (g) non-face to face customers and (h) those with dubious reputation as per public information available (i) Accounts of bullion dealers including sub-dealers and jewelers

However, only NPOs / NGOs promoted by United Nations or its agencies may be classified as low risk customer.

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

2.4 Customer Identification Procedure (CIP)
The policy clearly spells out that the Customer Identification Procedure is to be carried out at different stages i.e.

1. while establishing a banking relationship;
2. carrying out a financial transaction
3. or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship.

Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.).

For customers that are **natural persons**, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.

For customers that are **legal persons or entities**, the bank should (i) verify the legal status of the legal person/ entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution.

The branches should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are [Ref: Government of India Notification dated June 16, 2010 - Rule 9 sub-rule (1A) of PML Rules].

a) The Unique Identification Code for Customers across different banks enables for setting up a centralized KYC Registry. The Unique Customer Identification Code(UCIC) will help banks to identify Customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. Branches should open accounts to their customers under this UCIC only.

b) Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, branches should carry out full scale customer due diligence (CDD) before opening an account

c) When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship. [Ref: Government of India Notification dated June 16, 2010- Rule 9sub-rule (1D) of PML Rules].

d) It has been observed that some **close relatives**, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some branches as the **utility bills** required for address verification are not in their name. It is clarified, that in such cases, branches can obtain **an identity document and a utility bill** of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her.

Branches can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, branches should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

e) Branches should introduce a system of periodical **updation of customer identification data (including photograph/s)** after the account is opened.

The periodicity of such updation should not be less than once in ten years in case of low risk category customers, not less than once in eight years for medium risk category customers and not less than once in two years in case of high risk category customers.

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

g) The said indicative list furnished in Annex -I, shall not be treated as an exhaustive list as a result of which a section of public is being denied access to banking services.

h) In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, UIDAI has launched its e-KYC service. 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. Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules. In this connection, it is advised that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents (BCs). The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/BCs, which may be accepted as valid process for KYC verification.

2.5 Customer Identification Requirements – Indicative Guidelines

i) Walk-in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified.

However, if a 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 identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIUIND.

NOTE: 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.

ii) Trust/Nominee or Fiduciary Accounts

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

While opening an account for a trust, branches should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

iii) Accounts of companies and firms

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a **public company** it will not be necessary to identify all the shareholders.

iv) Client accounts opened by professional intermediaries

a) When the branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

b) Branch may hold **'pooled' accounts** managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the branch/ branches, the branch should still look through to the beneficial owners.

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

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

It is reiterated that branches should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality.

Further, any professional intermediary who is under any obligation that inhibits bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

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

a) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.

The decision to open an account for a PEP should be taken at the Zonal Office level. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

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

c) Further, branches should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

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

With the introduction of mobile phone / telephone / 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, branches may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards.

In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the branch /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.

vii) Accounts of proprietary concerns

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

a) Proof of the name, address and
b) activity of the concern, like

Registration Certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, Registration / Licensing Document issued in the name of the proprietary concern by the central government / State Government Authority / Department, Importer Exporter Code [IEC] issued to the Proprietary concern by the Office of the Directorate General of Foreign trade [DGFT].

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

c) These guidelines on proprietorship concerns will apply to all new customers, while in case of accounts of existing customers; the above formalities should be completed in a time bound manner and should be completed before December 31, 2010.

viii) Accounts of Salaried Employees

With a view to containing the risk of fraud, the branch need to rely on a certificate of identity as address proof issued by the employer only from corporate and other entities of repute and the branch should be aware of the competent authority designated by the employer to issue such a certificate / letter.

In addition to the certificate from the employer, branches should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering [PML] Rules [viz. passport, driving licence, PAN card, Voter's identity card etc.] or utility bills for KYC purpose for opening bank accounts of salaried employees of corporate and other entities.

Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act, 1949 and PML Rule, 2005.

2.6 Bank no longer knows the true identity

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

2.7 a) Accounts with Introduction

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

Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I of this policy, branch should open an account for him, subject to:

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

ii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed.

In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

KYC norms in the old accounts.

Branches/offices shall complete the implementation of KYC norms for all accounts and to issue confirmation to the controlling offices. While in-operative accounts could be kept out of the current exercise, an in-operative account should be subjected to the KYC procedures as and when any transaction comes up and is sought to be transferred to the operative category.

2.7 b) Small Accounts

In terms of Government of India, Notification No. 14/2010/F.No.6/2/2007-E.S, the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 has been amended.

As per this notification, 'small account' means a savings account in banking company where-
(i) The aggregate of all credits in a financial year does not exceed rupees one lakh;
(ii) The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
(iii) The balance at any point of time does not exceed rupees fifty thousand.

An individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –
(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

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

(iii) 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.

(iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents; and

(v) Foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents.

The Notification has also expanded the definition of 'officially valid document' of the PML Rules to include job card issued by NREGA duly signed by an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. It is further advised that where a bank has relied **exclusively** on any of these two documents, viz. NREGA job card or Aadhaar letter, as complete KYC document for opening of an account, the bank account so opened will also be subjected to all conditions and limitations prescribed for small account.

2.7 c) Operation of bank accounts & money mules

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

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

c) The operations of such mule accounts can be minimised if the guidelines on opening of accounts and monitoring of transactions are followed. Branches are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

2.8 Monitoring of Transactions

a) Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

High-risk accounts have to be subjected to intensified monitoring. Every branch should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Branches should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less than once in six months.**

b) Branches should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds [Ref: Government of India Notification dated June 16, 2010 -Rule 9, sub-rule (1B)]

2.9 Closure of accounts

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

2.10 Risk Management

The Board of Directors of the bank is ensuring that effective KYC programme is put in place by establishing appropriate procedures and effective implementation.

Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures.

Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

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

Branches should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking and mobile banking, that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Many branches 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. Branches are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.12 Prevention of Money-laundering Amendment Rules, 2009 Obligation of Banks

Government of India vide Notification No.13/2009/F.No.6/8/2009-ES dated November 12, 2009, has amended the Prevention of Money-laundering Rules, 2005. Branches / Offices are now required to note the following instructions for strict compliance.

1. Proper records of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency should be maintained..

2. Records of transactions should be maintained for a period of ten years from the date of transaction between the client and the banking company, financial institution or intermediary, as the case may be.

3. Furnishing of information in respect of transactions should be kept strictly confidential.

4. Should identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship at the time of commencement of an account-based relationship and in all other cases, i.e. the non-account based customer [walk-in customer] the branch/office shall verify the identity and the address while carrying out: (i) transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected [photograph need not be submitted by a client falling under this clause], or (ii) any international money transfer operations.

5. If a branch / office 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 branch should verify the identity and the address of the customer and also consider filing a Suspicious Transaction Report (STR).

6. Hitherto, the verification of identity of the client within a reasonable time after opening the account/execution of the transaction was permitted. But now this has been discontinued.

7. Every branch / office shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

8. No branch / office shall keep any anonymous account or account in fictitious names.

9. Where the client is an individual, he/she shall submit to the bank one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents in respect of the nature of business including financial status of the client as may be required by the bank .

10. Where the client is a juridical person (a person connected with law, judges, legal matters), the Bank shall verify that any person purporting to act on behalf of such client is so authorised and verify the identity of that person.

Branches/ offices are advised to strictly follow the amended provisions of PMLA Rules and ensure meticulous compliance to these Rules. The other salient features of the amendments, relevant to banks and financial institutions, are appended as Annexure-I.

The Compliance Cell at Head Office shall forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15th of the succeeding month.

2.13 Combating Financing of Terrorism - Unlawful Activities (Prevention) Act, 1967 – Obligation of the Bank

1. Branches have to update the consolidated list of individuals/entities as circulated by Reserve Bank of India and before opening any new account, it should be ensured that the name/s of the proposed customer does not appear in the list.
2. Further, branches/offices should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Branches /Offices have also been advised that full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Zonal Office/ Circle Office.

3. The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.
4. 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.
5. **Branches have to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009and ensure meticulous compliance to the Order issued by the Government.**
6. On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, they should ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts.
7. In terms of Para 4 of the Order, in regard to **funds, financial assets or economic resources or related services held in the form of bank accounts**, the RBI would forward the designated lists to the banks requiring them to:
   a) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.
   b) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the branches/offices shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail to pmla@csb.co.in for onward transmission to the UAPA nodal officer of RBI, Mumbai.
   c) In case, the match of any of the customers with the particulars of designated individuals/entities is **beyond doubt,** the branches/offices would prevent designated persons from conducting financial transactions, under intimation to pmla@csb.co.in. for onward transmission to Joint Secretary (IS.I), Ministry of Home Affairs.
   d) Branches shall also file a Suspicious Transaction Report (STR) with Zonal Office covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

2.14 Freezing of financial assets

   a) On receipt of the particulars as mentioned in paragraph 6(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

      branches are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.
   b) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.
   c) The order shall take place without prior notice to the designated individuals/entities.

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

1. U.N. Security Council Resolution 1373 obligates countries to freeze, without delay, the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.
2. 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.
3. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals/entities
4. The freezing orders shall take place without prior notice to the designated persons involved.

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

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

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

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

All orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all branches after receiving the same from RBI. **Branches/ Offices are advised to bring the provisions of the UAPA to the notice of the staff concerned and ensure strict compliance.**

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

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

2.18 Scanning of accounts:

Branches are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

2.19 Jurisdictions that do not or insufficiently apply the FATF Recommendations

Financial Action Task Force [FATF] was established in 1989 by the G7 Summit in Paris in response to large amounts of drugs money being laundered. It is an intergovernmental body that develops and promotes policies and concrete standards to combat money laundering and terrorist financing. Since its creation in 1989, United Nations Security Council Resolution 1617 urged the international community to implement the FATF Standards. Despite all these efforts, some countries achieve insufficient progress towards compliance.

Utmost care should be taken by branches to ensure to cross check all account opening applications and transactions carried out in the accounts wherein the customers are related to these countries.

In case transaction involving the names and addresses of any of such individuals/ entities belonging to the places mentioned above, is detected by the branch, the matter should be reported to PMLA Cell, Head Office [Email ID: pmla@csb.co.in] immediately for onward submission to Reserve Bank of India / Financial Intelligence Unit-India (FIU-IND) / other regulatory authorities.

2.20 Correspondent Banking

a) Correspondent banking is the provision of banking services by one bank (**the "correspondent bank**") to another bank (**the "respondent bank**"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through accounts, cheques clearing etc.

Bank should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance.

Similarly, bank should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while

laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval.

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

b) Correspondent relationship with a "Shell Bank"

Banks should refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Bank should not enter into relationship with shell banks and before establishing correspondent relationship with any foreign institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks.

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

2.21 Applicability to branches and subsidiaries outside India

The guidelines contained in this policy shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank.

In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

2.22 Wire Transfer

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

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

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

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

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

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

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

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

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.

Domestic wire transfers

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

ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50000/- (Rupees

Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

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

(iii) Exemptions

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

(iv) Role of Ordering, Intermediary and Beneficiary banks

(a) Ordering Bank

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

(b) Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer.

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

(c) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India.

The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

2.23 Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Rules under the Prevention of Money Laundering Act (PMLA), 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information.

(i) Maintenance of records of transactions

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

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

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

c) all 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,subrule (1) clause (BA) of PML Rules]

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

(ii) Information to be preserved

Branches / offices are required to maintain all necessary information in respect of transactions referred to in Rule 3 to permit reconstruction of individual transaction, including the following information:

the nature of the transactions;

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

the date on which the transaction was conducted; and

the parties to the transaction

(iii) Maintenance and Preservation of record

Branches and offices are required to maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 above.

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

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

c) It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.
These records are required to be preserved for ten years as is required under PMLA, 2002.

2.24 Cash Transaction Reports (CTR)

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

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

ii) **ii)** All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

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

iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

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

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

a) The CTR is generated in the format prescribed by Reserve Bank in Para 2.19(iv)(b) of Master Circular on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002 dated July 01, 2010;

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

d) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this Policy are scrupulously followed by the branch.

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

2.25 Suspicious Transaction Reports (STR)

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

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

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

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

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, branches shall consider the indicative list of suspicious activities contained HO Circular 205/209 dated 30.10.2009.

vi) Branches should not put any restrictions on operations in the accounts where an STR has been made. Branches 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.

2.26 Suspicious Transactions Reporting under PMLA

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

1. PMLA

The Prevention of Money Laundering Act, 2002 (PMLA) enacted to prevent money laundering and to provide for confiscation of property derived from, or involved in, money laundering.

PMLA, and rules notified there under, came into effect from 1st July, 2005.

As per Section 3 of PMLA, "whosoever, directly or indirectly, attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the **proceeds of crime** and projecting it as untainted property shall be guilty of offence of Money Laundering"

.

Applies to whole of India

Applies to Banks, Housing Finance Companies, Chit fund Companies, Intermediaries, Financial Institutions, NBFCs, Co-operative Banks & Money Changers

Scheduled offences defined

All cash or suspicious or unusual financial transactions and also underlying criminal activities covered

2. Proceeds of Crime

Any property derived or obtained directly or indirectly, by any person as a result of criminal activity relating to scheduled offences or the value of such property.

Whosoever directly or indirectly attempts to indulge *OR* knowingly assists *OR* knowingly is a party *OR* is actually involved ,in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering(Section 3) 3 to 7 years imprisonment and fine of Rs. 500,000.

3.Offences under PMLA

There are three schedules of offences covered under PMLA.

Part A:-

1. Certain offences under the Indian Penal Code, relating to **waging war** against the State.
2. Certain offences under the Narcotics Drugs and Psychotropic Substances Act 1985 relating to **drug trafficking**.
3. Certain offences under the Explosive Substances Act 1908.
4. Certain offences under the **Unlawful Activities** (Prevention) Act, 1967.
5. Counterfeiting currency notes or bank notes and using as genuine, forged or **counterfeit currency** notes or bank notes.

Part B:-

Certain offences under the following Acts where the value of criminal activity is above Rs. 3.00 mio:

1) Indian Penal Code
2) Arms Act, 1959 and Explosives Act, 1884
3) Wild Life (Protection) Act, 1972
4) Immoral Traffic (Prevention)Act, 1956
5) Prevention of Corruption Act, 1988
6) Antiquities and Arts Treasures Act, 1972
7) Securities and Exchange Board of India Act, 1992
8) Customs Act, 1962
9) Labour System (Abolition) Act, 1976 &
10) Child Labour (Prohibition and Regulation) Act, 1986
11) Transplantation of Human Organs Act, 1994
12) Juvenile Justice (Care and Protection of children) Act, 2000
13) Emigration Act, 1983, Passports Act, 1967 & Foreigners Act, 1946
14) Copyright Act, 1957 & Trade Marks Act, 1999
15) Information Technology Act, 2000
16) Biological Diversity Act, 2002
17) Protection of Plant Varieties and Farmers Rights Act, 2001
18) Environment Protection Act, 1980
19) Water (Prevention and Control of Pollution) Act, 1974
20) Air (Prevention and Control of Pollution) Act, 1981
21) Suppression of Unlawful Acts against Safety of Maritime Navigation and Fixed Platform on Continental Shelf Act, 2002

Part C :-

An offence which is the offence of cross border implications and is specified in: Part A, or Part B, without any monetary threshold, or the offences against property under Chapter XVII of the Indian Penal Code.

4. Suspicious Transaction

Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –

1. gives rise to a reasonable ground of suspicion that it may involve the **proceeds of crime**; or
2. appears to be made in circumstances of unusual or unjustified complexity; or
3. appears to have no economic rationale or bonafide purpose;
4. gives rise to a reasonable ground of suspicion that it may involve **financing of the activities relating to terrorism**

Transaction' includes deposit, 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.

5. Reporting Obligations of Banks under PMLA, 2002

Bank must maintain a record of all cash transactions, whether it is single or series of cash transactions integrally connected to each other, where such series takes place within a month, and All suspicious transactions, of any value, whether in cash or otherwise, in Indian or foreign currency Bank must furnish information of such transactions to FIU-IND through Head Office.

6. Preservation period of records of STRs

Bank must verify and maintain the records of the Identity of client, Address - current and permanent , Nature of business, and Financial Status.

The records must be maintained for a period of 10 Years from the date of cessation of such transactions

7. *Parameters for closure of Alerts*

The alerts generated for STR are based on the 17 rules implemented in the system which comprises 33 parameters suggested by IBA out of their 61 parameters. The verification of alerts are being done at desk level at HO-PMLA Cell on the basis of the attached rules as mentioned in the ANNEXURE-II. If any suspicious transactions are identified by the desk level officer the same is being forwarded to the Chief manager and from there to Asst.General Manager and finally to the Chief Compliance Officer(CCO). After getting the approval from CCO, STR is filed to FIU-IND and the remaining alerts are being eliminated

STR Statements to be submitted within 7 days of arriving at a conclusion that any transaction is of suspicious nature.

8.Powers of the FIU-IND

Section 13 of the Prevention of Money Laundering Act, 2002 confers following powers on the Director, FIU-IND to ensure compliance.

***"13** (1) The Director may, either of his own motion or on an application made by any authority, officer or person, call for records referred to in sub-section (1) of section 12 and may make such inquiry or cause such inquiry to be made, as he thinks fit.*

(2) If the Director, in the course of any inquiry, finds that a banking company, financial institution or an intermediary or any of its officers has failed to comply with the provisions contained in section 12, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may, by an order, levy a fine on such banking

company or financial institution or intermediary which shall not be less than Rs. 10,000 but may extend to Rs. 100,000 for each failure."

9. Enforcement authority and powers

Directorate of Enforcement is designated as the Regulating Authority under the Act. Powers of Enforcement Director are to

enter any premises of the bank/branch

issues summons to bank (all connected branches) conduct survey/inspection

inspect & retain the records or the property check & verify any bank transaction

call for information

place identification marks make inventory

record statements

break open the lock, box, locker, safe, almirah seize any record or property or evidence examine any person on oath

search any bank official arrest any person

10. Transaction Monitoring Processes

*KYC process does not start and end with opening of account*s

Transactions should be monitored depending on the risk sensitivity of the account.

Special attention is to be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

High risk accounts should be subjected to intensive monitoring.

High value transactions by non account holding customers also to be monitored carefully.

Suspicious Transactions Reports are to be filed with FIU-IND in respect of all suspicious transactions /activity finalized as such by the Principal Officer (KYC/AML) by Head Office.

Filing of STRs is based on assessment made by the Bank in the light of customer transactions/activity and Bank is under no obligation to prove or testify this at a later date to FIU-IND/other investigating agencies

11. Customer Information

Customers should neither be told nor given any room for doubts in their mind that while seeking additional information and the Bank is looking at their transactions / activity with suspicion. Such disclosure / indication is against the provisions of relevant Act / guidelines.

12. Reasons for "Suspicion" for banking companies .

- **Identity of client**
  - False identification documents
  - Identification documents which could not be verified within reasonable time
  - Accounts opened with names very close to other established business entities
  - **Background of client** :Suspicious background or links with known criminals
- **Multiple accounts**
  - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
  - Unexplained transfers between multiple accounts with no rationale
- **Activity in accounts**
  - Unusual activity compared with past transactions
  - Sudden activity in dormant accounts
  - Activity inconsistent with what would be expected from declared business

- **Nature of transactions**
  - Unusual or unjustified complexity
  - No economic rationale or bonafide purpose
  - Frequent purchases of drafts or other negotiable instruments with cash
  - Nature of transactions inconsistent with what would be expected from declared business
- **Value of transactions**
  - Value just under the reporting threshold amount in an apparent attempt to avoid

Reporting: Value inconsistent with the client's apparent financial standing.

13: <u>Some of the characteristics of a suspicious transaction.</u>

Involvement of funds in illegal activity

Intended to hide or disguise assets derived from illegal activities Designed to evade anti money laundering guidelines

No business or apparent lawful purpose

The sort in which the particular customer is not normally expected to engage in and for which, after examining available facts, satisfactory linkage is not obtained

Unusual characteristics or activities

Attempts to avoid reporting or record keeping requirements Provides insufficient or suspicious information

14. <u>Indicators for Detection of Suspicion Transactions</u>

1. Match of customer details with known criminals or persons with suspicious background
2. Customer has been the subject of a law enforcement inquiry
3. Customer who conducts transactions in a pattern consistent with criminal proceeds, e.g. in amounts consistent with a lottery scam, illegal immigration
4. Transaction involving a jurisdiction/area considered to be high risk from the money laundering or drug trafficking perspective.
5. Transaction is unnecessarily complex for its stated purpose
6. Unusual single or aggregate transfers in single/multiple days
7. Transaction is inconsistent with financial standing or occupation, or is outside the normal course of business for the customer in light of the information provided by the customer when conducting the transaction or during subsequent contact with the customer
8. Routing of transfer through multiple locations
9. "U-Turn" Transactions i.e. money passes from one person or more than one persons but it finally returns to the hands of the original sender
10. Multiple related transactions that are split to just below maximum cash limit or reporting requirements
11. The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer
12. Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the customer's business
13. The volume or frequency of transactions has no economic rationale or lawful purpose.
14. Customer who travels unexplained distances to conduct transactions.
15. Customer who offers false identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g., use of identification cards issued by different countries).
16. Customer who uses agents or associates where the nature of the relationship or transaction(s) make it difficult to identify the beneficial owner of the funds.
17. Customer networks; i.e. defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services
18. Common Unique IDs used by multiple customers
19. Common address/telephone used by multiple unrelated receivers
20. Customer conducts multiple cash transactions in a single day
21. Customer conducts transactions involving countries that are known for highly secretive banking and corporate law practices
22. Customer is hurried, nervous or evasive
23. Customer has vague knowledge about amount of money involved in the transaction
24. Customer is accompanied by unrelated individuals.
25. Suspicion that the customer is acting on behalf of a third party but not disclosing that information
26. Customer provides information that seems minimal, possibly false or inconsistent
27. Customer changes the information provided after more detailed information is requested
28. Customer is reluctant to go forward with a transaction after being informed that identification information will be required
29. Customer is reluctant to provide original ID
30. Customer makes inquiries or tries to convince staff to avoid reporting
31. Customer who offers different identifications or different identifiers (such as phone or address) on different occasions with an apparent attempt to avoid linkage of multiple transactions
32. Match of customer details with known terrorists or persons linked with terrorist organizations
33. Customer who receives transactions in a pattern consistent with financing of terrorism
34. Transaction involving a jurisdiction/area considered to be high risk from the terrorist financing perspective
35. There is no threshold limit for STRs
36. Attempted Transactions may be reported. Suspicious Transactions not necessarily linked to predicate offences
37. If suspicious transaction or activity involve a group of persons, natural or legal, file only ONE STR. STR is a case report-give total facts in STR.
38. STR Report shall be submitted within 7 days of confirmation of suspicion

15. Accounts already banned to open / operate

UNSCR enlisted individuals and entities and as notified by Reserve Bank of India.

Cash transactions during a calendar month, which are more than Rs.10 lakh and also those transactions, summation (credits and debits taken separately) of which exceeds Rs.10 lakh as well as all series of cash transactions integrally connected to each other.

Only transactions carried out on behalf of clients/customers excluding internal accounts of the bank.

all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or forgery of valuable security or document has taken place.

16. Civil Proceeding against the banking Official for CTR/STR reporting

Section 14 - No civil proceedings against banking companies & their official for CTR/STR reporting, but as per Section 13(2) ,Director,FIU-IND can impose fine on banks and as per **Section 24 - Burden of proof** on the accused.

17. Website for FIU-India for downloading more information on PMLA ,STR, CTR, CCR, etc,: http://fiuindia.gov.in ; http://www.un.org/sc/committees/1267/consolist.shtml

2.27 Counterfeit Currency Report [CCR]

Banks are responsible for providing genuine currency notes to the public that can be used by them with confidence. As circulation of fake notes has been increasing, as evidenced from the incidents of detection, individuals may come in possession of a counterfeit note without the knowledge of it being counterfeit and unintentionally become a conduit for circulation of the same by presenting it to a bank, business establishment, etc. Reporting of forged or counterfeit currency notes requires filing of FIR. In order to avoid consequent inconveniences, there is a tendency to under report such cases to the police / Reserve Bank of India.

In case any person in possession of fake notes tenders the same at a branch counter, the branch shall impound such notes and provide acknowledgement to the tenderer as per the current guidelines. Branch shall obtain approved ID document(s) of the tenderer (in the case of a customer, the bank would already have the necessary documents. For a non-customer, approved ID document or finger prints may be obtained).

Please note that information regarding the production, distribution or passing of counterfeit notes may be reported to local police.

Alternate reporting to FIU-IND on detection of counterfeit notes

Such instances shall be included in the Counterfeit Currency Report (CCR) and reported to Head Office, PMLA Cell for onward transmission of consolidated Statement to FIU-IND. New Delhi.

2.28 Non-Profit Organisation

Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO) as 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 under section 25 of the Companies Act, 1956.

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.

2.29 Reporting to Financial Intelligence Unit – India

In terms of the PMLA Rules, banks are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

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

The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for bank to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND.

The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.

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

2.30 Customer Education/Employee's Training/ Hiring of Employees a) Customer Education

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

b) Employee's Training

Bank must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

c)Recruitment / Hiring of Employees

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not

allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

2.31 Principal Officer of the Bank for KYC/ AML/ CFT compliance

a) Banks should appoint a senior management officer not below the cadre of Deputy General Manager to be designated as Principal Officer. Banks should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors.

Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.

He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism

b) Further, the role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there-under, as amended form time to time.

The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to FIU-IND.

c) With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

2.32 Evaluation of KYC Guidelines by Internal Audit and Inspection System

Zonal offices should periodically monitor strict compliance to the laid down policies and procedures at the branch level.

An independent evaluation of KYC guidelines for identifying High Value transactions would be required to be carried out buy Concurrent / Internal Auditors. They would be required to comment on the effectiveness of measures taken by the branches / level of implementation of KYC guidelines and prevention of money laundering at branches / offices.

A Review of the compliance of KYC and AML and CFT guidelines of the ban k as a whole shall be put up by the PMLA Cell to the Audit Committee of the Board [ACB] at quarterly intervals.

2.33 The importance of KYC norms to the employees

The employees of the bank will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff and management shall not provide advice or other assistance to individuals who are indulging in money laundering activities.

Dereliction of duty and avoidance of knowledge on KYC / AML / CFT / obligation of bank will lead to examination / fixation of staff accountability.

2.34 Certain occasions arousing suspicion on bank employees:

1. Unexplained shortage of significant amount of bank's funds reported on account of the same employee.
2. Frequently exceeding the discretionary power and allowing excess drawings to borrowers without proper justification / reporting to appropriate authority for control.
3. Reluctance to take job rotation / routine transfer
4. Employee does not avail of leave / take vacation.
5. Gross negligence of employee's willful blindness is reported repeatedly.
6. Life-style of the employee inconsistent with the known source of income.
7. Request for frequent high value DD purchases / transfer of high value funds by staff members.

2.35 Duties/ Responsibility and Accountability of employees

Personnel	Duties / Responsibilities
Officer in Charge of Accounts / Officer vested with authority to open new accounts	1. To interview the potential customer 2. To verify the introductory reference / customer profile. 3. To arrive threshold limits for each account, new as well as existing, and to exercise due diligence in identifying suspicious transactions. 4. To ensure opening of accounts in the names of terrorist individual / entities / banned organizations 5. To adhere to the [provisions of Foreign Contribution Regulatory Act 1976, Prevention of Money laundering Act 2005, Unlawful Activities Prevention Act. 6. To comply with the guidelines issued by the Bank from time to time in respect of opening and conduct of accounts
Principal Officer at branches / offices	1.To scrutinize and satisfy himself / herself that the information furnished in the account opening form / customer profile/ threshold limit/risk categorization are in strict compliance with KYC guidelines before authorizing / opening of account. 2.To certify in the Statement / Register regarding compliance with KYC guidelines and report all Suspicious Transactions and Counterfeit Currency Reports to appropriate authority in time.
Internal Inspectors / Concurrent Auditors / Inspecting Officials	To verify and report his comments on the effectiveness of measures taken by the branch/offices and level of implementation of KYC/AML/CFT guidelines
Controlling Authority	Prompt reporting of information regarding Suspicious Transactions / Counterfeit Currency Transactions to the law enforcing authority concerned in consultation with PMLA Cell, Head Office.

2.36 PMLA CELL [PREVENTION of Money Laundering Act Cell]

In light of the recent developments in global scenario, there has been an increasing recognition among financial institutions of the need for strengthening of the financial system to prevent its use for laundering proceeds of criminal activities.

Financial institutions / organizations around the world and in India have adopted various measures to address and tackle the issues involved.

THE Bank has set up Prevention of Money Laundering Act Cell [PMLA CELL] in the Operational Risk Management Department [ORMD] at Head Office.

Activities of PMLA Cell

1. Study of International Best Practices and Codes on Anti - Money Laundering (AML) and Combating Financing of Terrorism (CFT).
2. Correspondence with Government of India and its agencies like Central Economic Intelligence Bureau, Financial Intelligence Unit-India, and other Departments of RBI on AML / CFT related issues.
3. Follow up of the decisions taken by the Inter-Ministerial Co-ordination Forum for addressing issues relating to financing of terrorism such as Financial Intelligence Unit, Suspicious Transactions Reporting etc.
4. Review of guidelines issued to banks on 'Know Your Customer (KYC)' and 'Cash Transactions'.
5. Preparation of briefs for top management for meetings with various organizations / authorities.
6. Taking up issues with AML implications such as money transfer services with concerned authorities/organizations/RBI departments.
7. The cell will contribute material for the Management publications like Circulars/ Memos, guidelines, journals.
8. Taking follow-up action on points emanating from meetings of Board and Committees.
9. The Cell will also bring out every quarter a report on its important activities and submit quarterly / half- yearly /yearly reports to Audit Committee of the Board.
10. Issuance of Branch Circulars and Frequently Asked Questions and other publications for the benefit of staff members and others.
11. The cell is also represented in various Committees, Working Groups, and Forums etc.
12. Imparting training to the staff members on Best Practices and Codes on Anti - Money Laundering (AML) and Combating Financing of Terrorism (CFT).
13. Advising officers on measures required to prevent and detect money laundering in the branches / Offices
14. Providing general or specific information to the Board.
15. Submission of Compliance Certificates on KYC /AML, Risk Profiling, STR / CTR Returns.

****

ANNEXURE – I

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

Features	Documents
Accounts of individuals - Legal name and any other names used	1. Passport 2. PAN card 3. Voter's Identity Card 4. Driving license 5. Identity card (subject to the bank's satisfaction) **6.** Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank **7.** The letter issued by UIDAI containing details of name, address and Aadhaar number **8.** Job card issued by NREGA duly signed by an officer of the State Government **9. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process.**
Correct permanent address: any one document which provides customer information to the satisfaction of the bank will suffice	1. Telephone bill 2. Bank account statement 3. Letter from any recognized public authority 4. Electricity bill 5. Ration card **6.** Letter from employer (subject to satisfaction of the bank)
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	1. Certificate of incorporation and Memorandum & Articles of Association 2. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account 3. Power of Attorney granted to its managers, officers or employees to transact business on its behalf 4. Copy of PAN allotment letter 5. Copy of the telephone bill
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	1. Registration certificate, if registered 2. Partnership deed 3. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf 4. Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses 5. Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlors, beneficiaries and signatories - Names and addresses of the founder, the managers/ directors and the Beneficiaries Telephone/f ax numbers	1. Certificate of registration, if registered 2. Power of Attorney granted to transact business on its behalf 3. Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/ managers/ directors and their addresses 4. Resolution of the managing body of the foundation/association 5. Telephone bill
Accounts of Proprietorship concerns Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.	1. Proof of the name, address and activity of the concern Registration certificate (in the case of a registered concern) 2. Certificate / license issued by the Municipal authorities under Shop & Establishment Act, 3. Sales and income tax returns 4. CST / VAT 5. certificate / registration document issued by Sales Tax/ Service Tax/ Professional Tax authorities 6. License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, 7. Registration / Licensing Document issued in the name of the proprietary concern by the central government / State Government Authority / Department, Importer Exporter Code [IEC] issued to the Proprietary concern by the Office of the Directorate General of Foreign trade [DGFT].