APPENDIX: A
(CHapter 3: paragraph 3.5)

The Characteristics of an Ideal Financial Haven

Major Characteristics:

- No sharing of tax information with other countries.
- Availability of instant corporations.
- Corporate secrecy laws.
- Excellent electronic communications.
- Tight bank secrecy laws.
- Large tourist trades that can help explain major inflows of cash.
- Use of major world currency, preferably the US dollar, as the local money.
- A Government that is relatively invulnerable to outside pressure.
- High degree of economic dependence on the financial services sector.
- A geographic location that facilitates business travel to from rich neighbours.

Additional Characteristics\(^1\):

- Time zone location.
- A free-trade zone.
- Availability of a flag-of-convenience shipping registry.

---

\(^1\) UNDCP, 2001
APPENDIX:B

(CHAPTER 4: PARAGRAPH 4.5.8)

Major Terrorist Organizations:

- Abu Nidal Organization (ANO, or Black September, split from the PLO in 1974)
- Japan's Aum Supreme Truth (Aum Shinrikyo, known for the sarin gas attacks on Tokyo's subway system in 1995)
- Spain's Basque separatists (known as the ETA, a Spanish acronym for Basque Fatherland and Liberty)
- HAMAS (the Islamic Resistance Movement, operating in the West Bank areas of Israel and Jordan and dedicated to the destruction of the State of Israel)
- Hizballah (the Party of God, dedicated also to the destruction of Israel and the establishment of an Iranian style Islamic republic)
- Sri Lanka's Tamil Tigers (known as drug couriers moving heroin from Asia to western Europe)
- Bolivia's National Liberation Army (ELN, self-styled heirs to Che Guevara's legacy)
- Cambodia's Khmer Rouge (involved in heroin production in the Golden Triangle area of southeast Asia)
- The Popular Front for the Liberation of Palestine.
- Al-Qaeda (an umbrella group, fighting for a purer form of Islam, responsible for 1988 attacks on US embassies in Kenya and Tanzania and also for September 11, 2001 attack on W.T.C. New York (USA).
- India's anti-terrorism law, Prevention of Terrorism Act, 2002 (POTA) enlists certain terrorist organizations in its Schedule. Those organizations have been mentioned in Appendix C.
APPENDIX: C

Terrorist Organizations as declared so under India's Prevention of Terrorism Act, 2002 (POTA):

2. Khalistan Commando Force.
4. International Sikh Youth Federation.
5. Lashkar-E-Taiba/Pasbane-E-Ahle
10. United Liberation Front of Assam (ULFA).
12. People's Liberation Army (PLA).
17. Manipur People's Liberation Front (MPLF).
18. All Tripura Tiger Force.
20. Liberation Tigers of Tamil Eelam (LTTE).
21. Students Islamic Movement of India.
22. Deendar Anjuman.
23. Communist Party of India (Marxist-Leninist)-People's War, All Its Formations and Front Organizations.
24. Maoist Communist Centre (MCC), All Its Formations and Front Organizations.
APPENDIX: D

Guidelines on ‘Know Your Customer’ norms And Anti-Money Laundering Measures:

'Know Your Customer' Standards

1. The objective of KYC guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. Banks should frame their KYC policies incorporating the following four key elements:
   I. Customer Acceptance Policy;
   II. Customer Identification Procedures;
   III. Monitoring of Transactions; and
   IV. Risk management.

For the purpose of KYC policy, a ‘Customer’ may be defined as:

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and;
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.
Customer Acceptance Policy (CAP)

2. Banks should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.
   i. No account is opened in anonymous or fictitious/benami name(s);
   ii. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III ); customers requiring very high level of monitoring, e.g. Politically Exposed Persons may, if considered necessary, be categorized 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 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 categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
   v. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when
an account is operated by a mandate holder or where an account may be
opened by an intermediary in the 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 organizations etc.

Banks may prepare a profile for each new customer based on risk categorization.
The customer profile may contain information relating to customer’s identity,
social/financial status, nature of business activity, information about his clients’
business and their location etc. The nature and extent of due diligence will depend
on the risk perceived by the bank. However, while preparing customer profile
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 will be a
confidential document and details contained therein shall not be divulged for
cross selling or any other purposes.

For the purpose of risk categorization, individuals (other than High Net Worth)
and entities whose identities and sources of wealth can be easily identified and
transactions in whose accounts by and large conform to the known profile, may be
categorised as low risk. Illustrative examples of low risk customers could be
salaried employees whose salary structures are well defined, people belonging to
lower economic strata of the society whose accounts show small balances and low
turnover, Government departments & Government owned companies, regulators
and statutory bodies etc. In such cases, the policy may require that only the basic
requirements of verifying the identity and location of the customer are to be met.
Customers that are likely to pose a higher than average risk to the bank may be
categorized as medium or high risk depending on customer’s background, nature
and location of activity, country of origin, sources of funds and his client profile
etc. Banks 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 may include (a) non-resident customers, (b) high net worth individuals, (c) trusts, charities, NGOs and organizations receiving donations, (d) companies having close family shareholding or beneficial ownership, (e) firms with 'sleeping partners', (f) politically exposed persons (PEPs) of foreign origin, (g) non-face to face customers, and (h) those with dubious reputation as per public information available, etc.

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

**Customer Identification Procedure (CIP)**

3. The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural
persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annex-I for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers’ prudence and the legal requirements as per established practices If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

**Monitoring of Transactions**

4. 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. The bank 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 intensify monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Banks should ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, is reported to the appropriate law enforcement authority.

Banks should ensure that its branches continue to maintain proper record of all cash transactions (deposits and withdrawals) of Rs.10 lakh and above. The internal monitoring system should have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

**Risk Management**

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

Banks’ internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank’s own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard may be put up before the Audit Committee of the Board on quarterly intervals.

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

**Customer Education**

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

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

Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Further, marketing of these 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.

KYC for the Existing Accounts

8. Banks were advised vide our circulars DBOD.AML.BC.47/14.01.001/2003-04, DBOD.AML.129/14.01.001/2003-04 and DBOD.AML.BC.No.101/14.01.001/2003-04 dated November 24, 2003, December 16, 2003 and June 21, 2004 respectively to apply the KYC norms advised vide our circular DBOD. No. AML.BC.18/ 14.01.001/ 2002-03 dated August 16, 2002 to all the existing customers in a time bound manner. While the revised guidelines will apply to all new customers, banks should apply the same to the existing customers on the basis of materiality and risk. However, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the CDD measures. Banks may consider applying monetary limits to such accounts based on the nature and type of the account. It may, however, be ensured that all the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to
minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. Banks may also ensure that term/recurring deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and subjected to revised KYC procedures. 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 may 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.

**Applicability to branches and subsidiaries outside India**

9. The above guidelines shall also 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.

**Appointment of Principal Officer**

10. Banks may appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.
APPENDIX- E
Customer Identification Requirements – Indicative Guidelines

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and the 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.

Accounts of companies and firms

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

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance policy. Banks should also subject such accounts to enhanced monitoring on an ongoing
basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

**Accounts of non-face-to-face customers**

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

**Correspondent Banking**

Correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank'). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank’s management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory
framework in the correspondent's/respondent’s country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

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

Anti-Money Laundering Guidelines for Authorised Money Changers
December 02, 2005

1. Money Laundering

The offence of Money Laundering has been defined in Section 3 of the Prevention of Money Laundering Act, 2002 (PMLA) as "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". In common man’s language, Money Laundering can be called a process by which money or other assets obtained as proceeds of crime are exchanged for "clean money" or other assets with no obvious link to their criminal origins.

2. Anti-Money Laundering Guidelines

The purpose of prescribing Anti-Money Laundering Guidelines is to prevent the system of Authorised Money Changers (AMCs) engaged in the purchase and / or sale of foreign currency notes/Travelers cheques from being used for money laundering. Therefore, Anti-Money Laundering (AML) measures should include
a. Identification of Customer according to "Know Your Customer" norms,
b. Recognition, handling and disclosure of suspicious transactions,
c. Appointment of Money Laundering Reporting Officer (MLRO),
d. Staff Training,
e. Maintenance of records,
f. Audit of transactions.

The following paragraphs contain broad guidelines to enable AMCs to formulate and put in place a proper policy framework for AML measures.
3. **Know Your Customer (KYC) – Identification of Customers**

All transactions should be undertaken only after proper identification of the customer. Photocopies of proof of identification should invariably be retained by the AMC after verifying the document in original. Full details of name and address as well as the details of the identity document provided should also be kept on record. If a transaction is being undertaken on behalf of another person, identification evidence of all the persons concerned should be obtained and kept on record.

4. **Purchase of Foreign Exchange**

a) For encashment of foreign currency notes and/or Travelers Cheques upto USD 500 or its equivalent, production of passport need not be insisted upon and any other suitable document of identification like ration card, driving licence etc. can also be accepted.

b) For verification of the identity of customer for encashment in excess of USD 500 or its equivalent, a photo identity document such as passport, driving licence, PAN Card, voter identity card issued by the Election Commission, etc. should be obtained.

c) Requests for payment of sale proceeds in cash may be acceded to the extent of USD 1000 or its equivalent per transaction. All encashment within one month may be treated as single transaction for the purpose. In all other cases AMCs should make payment by way of 'Account Payee' cheque / demand draft only.

d) Where the amount of forex tendered for encashment by a non-resident or a person returning from abroad exceeds the limits prescribed for Currency Declaration Form (CDF), the AMC should invariably insist for production of declaration in CDF.
5. **In all cases of sale of foreign exchange, irrespective of the amount involved**

For identification purpose the passport of the customer should be insisted upon. The sale of forex should be made only on personal application and identification. Payment in excess of Rs. 50,000/- towards sale of foreign exchange should be received only by account payee cheque / demand draft. All purchases by a person within one month may be treated as single transaction for the purpose. Encashment Certificate, wherever required, should also be insisted upon.

6. **Establishment of business relationship**

Relationship with a business entity like a company / firm should be established only after obtaining and verifying suitable documents in support of name, address and business activity such as certificate of incorporation under the Companies Act, 1956, MOA and AOA, registration certificate of a firm (if registered), partnership deed, etc. A list of employees who would be authorised to transact on behalf of the company/ firm and documents of their identification together with their signatures, should also be called for. Copies of all documents called for verification should be kept on record.

7. **Suspicious Transactions**

The AMC must ensure that its staff is vigilant against money laundering transactions at all times. An important part of the AML measures is determining whether a transaction is suspicious or not. A transaction may be of suspicious nature irrespective of the amount involved. Some possible suspicious activity indicators are given below:

- Customer is reluctant to provide details/documents on frivolous grounds.
- The transaction is undertaken by one or more intermediaries to protect the identity of the beneficiary or hide their involvement.
Large cash transactions.

Size and frequency of transactions is high considering the normal business of the customer.

Change in the pattern of business transacted.

The above list is only indicative and not exhaustive.

8. Appointment of a Money Laundering Reporting Officer (MLRO)

a. An MLRO may be appointed by every AMC for monitoring transactions and ensuring compliance with the AML Guidelines issued by the Reserve Bank from time to time. The MLRO will also be responsible for reporting of suspicious transaction/s to the Financial Intelligence Unit (FIU). Any suspicious transaction/s, if undertaken, should have prior approval of MLRO.

b. The MLRO shall have reasonable access to all the necessary information/documents, which would help him in effective discharge of his responsibilities.

c. The responsibility of the MLRO may include:
   - Putting in place necessary controls for detection of suspicious transactions.
   - Receiving disclosures related to suspicious transactions from the staff or otherwise.
   - Deciding whether a transaction should be reported to the appropriate authorities
   - Training of staff and preparing detailed guidelines / handbook for detection of suspicious transactions.
   - Preparing annual reports on the adequacy or otherwise of systems and procedures in place to prevent money laundering and submit it to the Top Management within 3 months of the end of the financial year.
9. Reporting of Suspicious Activity

To the extent possible, all suspicious transactions should be reported to the MLRO before they are undertaken.

- Full details of all suspicious transactions, whether put through or not, should be reported, in writing, to the MLRO.
- Any transaction which seems suspicious may be undertaken only with prior approval of MLRO.
- If the MLRO is reasonably satisfied that the suspicious transaction has / may have resulted in money laundering, he should make a report to the appropriate authority viz. the FIU.

10. Staff Training

All the managers and staff of the AMC must be trained to be aware of the policies and procedures relating to prevention of money laundering, provisions of the PMLA and the need to monitor all transactions to ensure that no suspicious activity is being undertaken under the guise of money changing. The steps to be taken when the staff come across any suspicious transactions (such as asking questions about the source of funds, checking the identification documents carefully, reporting immediately to the MLRO, etc.) should be carefully formulated by the AMC and suitable procedure laid down. The AMCs should have an ongoing training programme for consistent implementation of the AML measures.

11. Audit/Compliance

The concurrent auditor should check all transactions to verify that they have been done in compliance with the anti-money laundering guidelines and have been reported as required. Compliance on the lapses, if any, recorded by the concurrent
auditor should be put up to the Board. A certificate from the Statutory Auditor on the compliance with AML guidelines should be obtained at the time of preparation of the Annual Report and kept on record.

12. Maintenance of records

The following documents should be preserved for a minimum period of five years.

- Records including identification obtained in respect of all transactions.
- Statements / Registers prescribed by the Reserve Bank from time to time.
- All Inspection / Audit / Concurrent Audit Reports.
- Annual reports of the MLRO submitted to the Top Management in terms of paragraph 8 above.
- Details of all suspicious transactions reported in writing or otherwise to the MLRO.
- Details of all transactions involving purchase of foreign exchange against payment in cash exceeding Indian Rupees 10,00,000 from inter-related persons during one month.
- All correspondence/ reports with the appropriate authority in connection with suspicious transactions.
- References from Law Enforcement Authorities, including FIU, should be preserved until the cases are adjudicated and closed.