Chapter III

KYC norms/AML measures

Objective:

The objective of KYC guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

Apart from this Bank realizes the need for a well defined customer acceptance, customer care and customer severance policy to ensure prompt and inclusive services to all customers within the prescribed regulatory framework as well as defined processes of the Bank. In this regard, Damodaran Committee on Customer Service, constituted by the Reserve Bank of India, has also recommended certain important themes which have been incorporated to design the policy towards comprehensive coverage and implementation of customer acceptance, customer care/customer service and customer severance in the bank. Through this Policy the bank shall ensure that the recommendations of the Damoradan Committee as well as relevant regulatory and other requirements are implemented in letter and spirit.

Definition of a 'Customer':

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

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

Guidelines:

1. Branches 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.
2. Branches shall 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 shall ensure that the provisions of Foreign Contribution and Regulation Act, (FCRA) 1976 as amended from time to time wherever applicable are adhered to strictly. They shall desist from opening accounts in the name of banned organizations and those without registration. In this connection, branches shall be guided by the circulars issued from time to time.

Key Elements of the KYC Policy

Following are four key elements of our KYC policy:

(a) Customer Acceptance and Customer Severance Policy

(b) Customer Identification Procedures;

(c) Monitoring of Transactions;
(d) Risk Management

1. Customer Acceptance Policy (CAP)

(a) **Branches must ensure that no account is opened**:

* In anonymous or fictitious/ benami name(s);
* In the names of persons with a criminal background and/or having connections with terrorist organizations.
* No transaction or account based relationship is undertaken without following the CDD procedure.
* The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
* CDD Procedure is followed for all the joint account holders, while opening a joint account.
* Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
* Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
*A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

(b) **Risk Perception:**

1. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception
2. Risk categorisation shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and information about the clients' business and their location etc.

No financial sector business is immune from the activities of criminal elements. The level of Money Laundering Risk that Bank is exposed to by a customer relationship depends on:

o Type of the customer and nature of business o Type of product/service availed by the customer o Country where the customer is domiciled

Based on the above criteria, the customers are classified into three Money laundering Risk levels as follows:

High Risk - who are engaged in certain professions where money-laundering possibilities are high. The indicative List of High risk customers is furnished

hereunder:

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. Customers based in high risk countries / jurisdictions or locations **(Annexure I)**
8. 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;
9. Non-resident customers and foreign nationals
10. Embassies / Consulates
11. Off-shore (foreign) corporation / business
12. Non face-to-face customers
13. High net worth individuals
14. Firms with 'sleeping partners'
15. Companies having close family shareholding or beneficial ownership
16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
17. 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.
18. Investment Management/ Money Management Company / Personal Investment Company.
19. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
21. Trusts, Charities, NGOs/NPOs (especially those operating on a cross-border basis) unregulated clubs and organizations receiving donations (excluding NPOs / NGOs promoted by United Nations or its agencies).
22. Money Service Business: including seller of: Money Orders / Travellers' Checks / Money Transmission / Check Cashing / Currency Dealing or Exchange.
23. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks / cash pay roll checks).
24. Gambling / gaming including "Junket Operators" arranging gambling tours.
25. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
26. Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries).

27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
28. Customers that may appear to be Multi level marketing companies etc. Opening of above type of accounts shall be permitted by Regional Offices only.

C. **Correspondent Banks:**

Correspondent banking is the provision of banking services by one Bank (the "correspondent bank") to another Bank (the "respondent bank"). Such relationships shall be established by a committee headed by Chairman & Managing Director and consisting of Executive Director, GM (ID), GM (Inspection) and GM (Planning & Development.). 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 which 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.

Bank 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. Extreme caution must be exercised while establishing/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.

It must be ensured that our 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.

Medium Risk:

The indicative List of Medium risk customers is furnished hereunder:

1. Non-Bank 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 cafe, IDD call service, phone cards, phone center
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers

14. Cash-Incentive Business such as Restaurants, retail shops, parking garages, fast food stores, movie theaters etc.
15. Sole practitioners or Law Firms (small, little known)
16. Notaries (small, little known)
17. Secretarial Firms (small, little known)
18. Accountants (small, little known firms)
19. Venture capital companies.

These types of accounts shall be opened with prior approval of Regional Offices only. The list of medium risk countries is furnished in **Annexure II**

C. Low Risk:

- All the customers who are not High/ Medium Risk customers are low risk customers. These are the type of customers whose identity and source of wealth can be easily identified and the transactions in whose accounts by and large conform to the known profile
- Salaried employees whose salary structures are well defined
- People belonging to low economic strata of the society whose accounts show small balances and low turnover.
- Government Departments and Government owned companies, regulators and statutory bodies etc.,
- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment).
- Customers with long term and active business relationship with the Bank (who are not coming under High / Medium Risk)
- NPOs / NGOs promoted by United Nations or its agencies.

Branches should prepare a profile for each customer based on risk categorization as per **Annexure-3.**

The products and services are also to be categorized in addition to existing system of categorizing the customers as high/ medium/ low risk as above. The indicative list of high/ medium risk products and services is given hereunder

INDICATIVE LIST OF HIGH RISK PRODUCTS & SERVICES:

1. Electronic funds payment services such as electronic cash (e.g. stored value and pay roll cards) Funds transfers (domestic and international), etc.
2. Electronic Banking
3. Private Banking (domestic and international)
4. Trust and Asset Management Services
5. Monetary instruments such as Travelers' Cheque
6. Foreign Correspondent Accounts
7. Trade Finance (such as letters of credit)
8. Special use or concentration accounts
9. Transactions undertaken for non-account holders (occasional customers)
10. Provision of safe custody and safety deposit boxes
11. Currency Exchange Transactions
12. Project Financing of sensitive industries in high-risk jurisdictions
13. Trade Finance Services and transactions involving high-risk jurisdictions
14. Services offering anonymity or involving third parties

15. Services involving banknote and precious metal trading and delivery
16. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

INDICATIVE LIST OF MEDIUM RISK PRODUCTS & SERVICES

1. Lending activities, particularly loans secured by cash collateral and marketable securities and
2. Non-deposit account services such as Non-deposit investment products and insurance

Apart from the risk categorization of the countries, the Banks should categorize the geographies / locations within the country on both ML and TF risk. The TF risk of a location is more relevant if the utilization of money or cash withdrawal is taking place in locations with known terrorist incidents. Priority needs to be given on identification of locations (Pin Codes or Districts) with high or very high TF risk to detect TF related STRs.

Customer should be subject to higher due diligence if following criteria falls under "high risk" geographies.

- Country of nationality (Individuals)
- Country of residential address (Individuals)
- Country of incorporation (Legal entities)
- Country of residence of principal shareholders / beneficial owners (Legal entities)
- Country of business registration such as branch/liaison/project office
- Country of source of funds
- Country of the business or correspondence address
- Country with whom customer deals (e.g. over 50% of the business - trade, etc.)

Periodical Review of Risk Categorization of Customers:

All branches shall ensure maintaining and updating of customer risk profile on a continuous basis. A review of risk categorization of customers should be carried out at a periodicity of not less than once in six months.

Policy framework around Customer Severance:

1. The branches shall ensure implementation of the well laid guidelines and processes in relation to Customer Severance situations e.g. account closure, loan termination, loan foreclosure etc. The relevant processes for account closure shall be followed in letter and spirit in all possible instances e.g. either customer induced or bank induced.
2. In cases of customer induced account closure the bank shall, as a prudent practice, attempt to understand the underlying issues, if any leading to the separation. The Bank shall make all reasonable efforts to retain the customer by eliminating the product / service issues, if any. This shall be used to bridge gaps in process and service, if any.
3. Under all circumstances, the bank shall honour the customer's free will and ensure hassle-free closure of account within the framework of extant regulatory guidelines.
4. The bank shall carry out review of relationship at regular frequency. In the event customer's account behaviour is in contravention to the extant regulatory guidelines e.g. AML, Transaction pattern not matching with the profile etc., the bank shall take necessary steps to intimate the customer with a request to provide evidences in support of transaction pattern / account behaviour etc. In the event that the customer is unable to provide appropriate evidences or the customer is not traceable beyond a reasonable time-frame, bank will take steps to cease the relationship by obtaining due internal approvals and by issuing notice. It shall be ensured that there is no tipping off to the customer.
5. Drastic measure like closing of accounts is to be taken only after sending out sufficient

discernible warning signals to the customers having regard to the level of customer education and public awareness of the subject. In all such cases, where account holders are either not responding over a period of time/not found at the given addresses, branches may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

6. The Bank shall ensure comprehensive implementation of the above policy as well as review of the same at regular interval through Standing Committee on Customer Service, Customer Service Committee of the Board and the Board of Directors. This shall ensure strengthening the framework of Customer Acceptance, Customer Care, Customer Service and Customer Severance.

2. <u>Customer Identification Procedures</u>:

While undertaking customer identification, bank shall ensure that:

(a) Decision-making functions of determining compliance with KYC norms shall not be outsourced.

(b) Introduction shall not be sought while opening accounts.

(c) The customers shall not be required to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address.

The first requirement of knowing your customer for **anti-**money laundering purposes is to be satisfied that who he/she claims to be a prospective customer.

The second requirement of knowing the customer is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake **or** any expected, or predictable pattern of transaction.

Verification of identity means it has been decided by the Reserve Bank that ' simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering the terrorist financing risks involved.

Customer categorized as low risks expresses inability to complete the documentation requirement on account of any reason that the bank considers genuine and where it is essential not to interrupt the normal conduct of business, the regulator may permit the reporting entity to complete the verification within a period of 6 months from the date of establishment of relationship.

<u>Periodical Review/Updation of Customer Identification Data:</u>

A system of periodical updation of customer identification data (including photograph/s) after the account is opened shall be introduced as under:

- Branches would need to continue to carry out on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.
- Full KYC exercise will be required to be done at least every two years for high risk individuals and entities.
- Full KYC exercise will be required to be done at least every ten years for low risk and at least every eight years for medium risk individual and entities.

> **The periodicity of updation of documents is to be done along with client's due diligence on annual basis**

It has been decided by RBI to dispense with the requirement of positive confirmation as indicated above, in respect of medium and low risk customers is dispensed with.

Physical presence of the clients may, however, not be insisted upon at the time of such periodic updation.

> Fresh photographs will be required to be obtained from minor customer on becoming major.

> Do not insist on physical presence of the customer at the time of periodic updating.

> Do not seek fresh documents if an existing KYC compliant customer of a bank desires to open another account in the bank.

> Do not seek fresh proof of identity and address at the time of periodic updation from the customer who are categorized as 'low risk' in case of no change in status with respect to their identity and address.

Necessary checks shall be applied 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.

Branches shall not open an account where they are unable to apply appropriate customer due diligence measures i.e., branch 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 furnished to the bank. However, it shall be ensured that no harassment is caused to the customer in the process. Further, decision in such cases should be taken by the branch head only, after taking into consideration all the relevant facts.

Branches may adopt a risk-based approach to KYC requirements. Consequently, there will be circumstances when it will be both necessary and permissible to apply commercial judgment to the extent of the initial identification requirements. Decisions need to be taken on the number of verification parameters within a relationship, the identification evidence required, and when additional checks are necessary. The process of confirming and updating identity and address, and the extent of additional KYC information collected shall be an ongoing process.

Identity generally means a set of attributes which together uniquely identify a natural or legal person.

Identification evidence should usually be verified for:

- the named account holder(s)/the person in whose name an investment is registered;
- any principal beneficial owner of funds being invested who is not the account holder or named investor (Detailed procedure to be followed is furnished in our Circular No280-2014-BC-P&D-87 dated 8.9.2014)
- the principal controller(s) of an account or business relationship i.e. those who regularly give instructions; and
- any intermediate parties e.g. where an account is managed or owned by an intermediary.

<u>Identification Procedures: General Principles:</u>

A Branch should establish to its satisfaction that it is dealing with an individual or an entity and obtain identification evidence sufficient to establish that the applicant is that individual or entity.

When reliance is being placed on any third party to identify or confirm the identity of any

applicant, the overall legal responsibility to ensure that the procedures and evidence obtained are satisfactory, rests with the account holding branch.

Certification and Copying Identification Documents:

To guard against the dangers of postal intercept and fraud, prospective customers should not be asked to send originals of valuable personal identity documents, e.g. passport, identity card, driving licence, etc., by post.

Certified copies of identification evidence should be dated, and signed "original seen". In situations where a good reproduction of photographic evidence of identity cannot be achieved, the copy should be certified as providing a good likeness of the applicant.

Officer supervising the department may do the above certification.

Information to be collected for Customer Identification:

Information collected at the outset for customer identification purpose to include-

i) the purpose and reason for opening the account or establishing the relationship
ii) the anticipated level and nature of the activity that is to be undertaken
iii) the expected origin of the funds to be used within the relationship
iv) Details of occupation / employment to be sought for bank accounts and sources of wealth or income will be required for some banking relationships.

Features to be verified and documents that may be obtained from customers.

Branches / Offices are advised to note the following for compliance:

RBI , has clarified that the discretion given to the Banks in the clause " Any document notified by Central Govt" stands withdrawn and it should be "officially valid document". Further, RBI has clarified the list of officially valid documents as:

1. Passport,
2. PAN card,
3. Driving license,
4. Voter's Identity Card,
5. Job Card issued by NREGA and
6. Letter issued by UIAI.

Only the documents mentioned in SL No 1 to 6 above are only officially valid documents.

Relaxation for low risk customers:

If a person does not have any of the OVD mentioned above , but if is categorised as 'low risk' by the Banks, then he/she can open a bank account by submitting any one of the following documents:

A) Identity card with applicant's photograph issued by Central Govt/State Govt Depts , Statutory/Regulatory Authorities, PSUs,Scheduled Commercial Banks and Public Financial Institutions:

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

In case a customer categorised as 'low risk'is unable to submit the KYC documents due to genuine reasons, she/he may submit the documents to the bank within a period of six months from the date of opening account.

In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the documents at (i) and (ii) of proviso to rule 2
(d) for the purpose of identity and proof of address.

1. Indicative list of documents as "proof of identity" and "proof of address" provided by Department of Financial Services, Ministry of finance, Govt. of India is enclosed, which can be adopted while opening SB Accounts of individuals. The list is enclosed as **Annexure 6.**

2. It is sufficient to obtain one document for proof of identity and one document for proof of address. In case, the documents submitted by prospective account holder contain both identity and current address of the party, separate documents need not be insisted.

3. In case of non-individual entities, documents as mentioned in RBI Master Circular **(Our Circular No. 280-2014-BC-P&D-87 dated 08.09.2014)** shall be obtained. In addition to complying with KYC norms of non-individual entities, the authorized signatories (Director/ partner/ Trustee/ Manager etc.,) of the entity shall also be subjected to Customer identification procedure.

RBI has clarified that the discretion given to banks in the clause " any documents notified by central govt" stands withdrawn and it should be "officially valid document" (Passport, PAN card, Driving license,Voter's identity card, Job card issued by NREGA and letter issued by UIAI.) only these documents be accepted as proof of identity and documents accepted as proof of residence

5. Branches should invariably verify the Xerox copy of the document with the original and certify on the Xerox copy of the document that "Verified with original" under the signature of authorized official of the Branch.

6. Wherever, the photo on the document is not scanned / laminated but pasted, it should be ensured that round stamp of the authority issuing the document is affixed on the document in such a way that round stamp is partially appearing on the photo, thus avoiding tampering / misuse of document.

With regard to obtaining of two sets of KYC documents, i.e., one each for identity and address proof, the following are revised guidelines:

Single document for proof of identity and proof of address.

There is no requirement of submitting two separate documents for proof of identity and proof of address. If the officially valid document submitted for opening a document has both, identity and address of the person, there is no need for submitting any other documentary proof.

a) If the address on the document submitted for identity proof by the prospective customer is the same as that declared by him/ her in the account opening form, the document may be accepted as a valid proof of both identity and address (passport, PAN Card with covering letter, Driving Licence, Voter's ID Card etc.)

b) in case the proof of address furnished by the customer is not the local address or address where customer is currently residing, the Bank may take a declaration of the local address on which all correspondence will be made by the Bank with the customer. No proof is required to be submitted for such address for correspondence/local address.

Harmonisation of KYC norms for Foreign Portfolio Investors (FPI)

Reserve Bank of India in consultation with Government of India, has decided to simplify the KYC norms in case of FPIs.

1. FPIs have been categorized by SEBI based on their perceived risk profile as detailed in

Annex-VII. Such eligible / registered FPIs may approach a Bank for opening a Bank account for the purpose of investment under Portfolio Investment Scheme [PIS] for which, KYC documents prescribed by the Reserve Bank of India [as detailed in Annex-VIII] would be required. For this purpose,Banks may rely on the KYC verification done by the third party [i.e. the Custodian/SEBI Regulated Intermediary] subject to the conditions laid down in Rule 9 [2] {[a] to [e] }of the Rules.

2. In this regard, SEBI has been requested to advise Custodians/Intermediaries regulated by them to share the relevant KYC documents with the Banks concerned based on written authorization from the FPIs. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to the Custodian/Regulated Intermediaries may be transferred to the concerned Bank through their authorized representative. While transferring such documents, the Custodian/Regulated Intermediary shall certify that the documents have been duly verified with the original or notarized documents have been obtained, where applicable. In this regard a proper record of transfer of documents both at the level of the Custodians/Regulated Intermediary as well as at the Bank, under signatures of the officials of the transferor and transferee entities may be kept. While opening bank accounts for FPIs in terms of above procedure, Banks may bear in mind that they are ultimately responsible for the customer due diligence done by the third party [i.e. Custodian/Regulated Intermediaries] and may need to take enhanced due diligence measures, as applicable, if required. Further, Banks are required to obtain undertaking from FPIs or Global Custodian acting on behalf of the FPI to the effect that as and when required, the exempted documents as detailed in Annex VIII will be submitted.

3. It is further advised that to facilitate secondary market transactions, the Branches may share the KYC documents received from the FPI or certified copies received from a custodian/Regulated Intermediary with other Banks/Regulated market intermediaries based on written authorization from the FPI.

4. The provisions of this circular are applicable for both new and existing FPI clients. These provisions are applicable only for PIS by FPIs. In case of FPIs intend to use the Bank account opened under the above procedure for any other approved activities [i.e. other than PIS], they would have to undergo KYC drill as prescribed in RBI Master circular DBOD AML BC No.24/2 Circular No.157-2014-BC-P&D-44/31- 05-2014 14.01.001/2013-14 dated July 1, 2013 on Know Your Customer [KYC] norms / Anti-Money Laundering [AML] standards/Combating of Financing of Terrorism [CFT] /Obligation of Banks under PMLA, 2002

All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Shifting of Bank accounts to another Centre - Proof of Address:

- Branches may transfer existing KYC compliant accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address subject to submitting proof of address within a period of six months. (This shall be monitored by the transferee branch by putting a Low Severity Memo.)
- Branches should intimate their customers that in the event of change in address due to relocation / any other reason, they should intimate the new address to the Branch within two weeks of such a change. While opening new account and while periodically updating KYC data, an undertaking to this effect should be obtained.

Introduction not Mandatory for opening accounts:

Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions, branches should not insist on introduction for opening bank accounts of customers.

While opening the accounts of Non-Individuals (Proprietorship / Partnership / Companies / Trust / Association / Society etc., in addition to complying with the Customer Identification Procedure relating to Non-Individuals Entities, the individuals purporting to act on behalf of that entity shall also be subjected to Customer Identification Procedure. By adhering to the above guidelines, branches shall ensure that no account is opened in anonymous / fictitious / benami name and banking system is not utilized for Money Laundering and to finance Terrorism.

In cases where some close relatives, e.g. wife, son, daughter, parents etc. live with their husband, father/mother and son, as the case may be, 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 staying with him / her. The whole exercise is to keep in mind the spirit of instructions issued by the Reserve Bank of India and avoid undue hardships to individuals who are otherwise classified as Low Risk Customers.

Individual Non-Resident Accounts

Accounts to be opened on the basis of the following documents: - Passport & Residence Visa- Copies of these documents sighted in original by the bank official or duly attested by Banker/Notary Public/Indian Embassy/ Employer to the satisfaction of the bank.

Accounts of Foreign students studying in India:

Branches shall open accounts of Foreign students studying in India under "NRO category" only as they are treated as "Non-Resident".

The opening of the accounts by individual/s of Bangladesh Nationality shall be allowed by the branches , subject to satisfying itself that the individual/s hold a valid VISA and valid residential permit issued by Foreigner Registration Office(FRO)/Foreigner Regional Registration Office (FRRO) concerned.

STUDENTS WITH PAKISTAN NATIONALITY WILL NEED PRIOR APPROVAL OF RESERVE BANK OF INDIA FOR OPENING THE ACCOUNT

Foreign students have been allowed a time of one month for furnishing the proof of local address.

Minor accounts

Often a family member or guardian would open an account for a minor. In cases where the adult opening the account does not already have an account with the Branch, the identification proof for that adult or any other person who will operate the account should be obtained. In case of self operated minor accounts in addition to the photograph and proof of age, the documents required to establish the identity and address as applicable in the case of individual be obtained.

Married Woman Accounts

As part of Customer Identification Procedure, while opening / transferring accounts of newly married women and allowing conversion of name & signature in the existing accounts of women upon marriage, Marriage Certificate, Notarised Affidavit or Clear photograph of the wedding and

Address proof of the groom etc. along with additional information in prescribed formats are to be obtained.

Joint Account

In case of joint accounts, applicants who are not closely related to each other (as can be inferred from the Account opening form) would require to establish their identity and address independently.

Societies/ Associations / Clubs

In the case of applications received on behalf of clubs or societies, Branches should take reasonable steps to satisfy themselves as to the legitimate purpose of the organization by going through the constitution. The identity of the authorized signatories should be verified initially in line with the requirements for personal customers. When signatories change, care should be taken to ensure that the identity of any new signatories has been verified.

The following documents are to be obtained for opening accounts of Clubs, Societies and Associations wherever applicable:

- Resolution for opening of the account
- A copy of Bye-laws
- Copy of certificate of registration in the case of registered clubs, societies and associations.

Professional Intermediaries:

When a 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. Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches may also maintain 'pooled' accounts managed by lawyers/charted 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, the branch should still look through to the beneficial owners.

Reliance on Third Party due diligence

For the purpose of identifying verifying the identity of customer at the time of commencement of an account based relationship, reporting entity may rely on a third party subject to the conditions.

(a) Reporting entity immediately obtain necessary information of such client due diligence carried out by the third party.

(b) the reporting entity takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence will be made available from the third party upon request without delay.

(c) the reporting entity is satisfied that such third party is regulated supervised or monitored for and has measures in place for compliance with client due diligence and record keeping requirement in line with the requirement and obligations under the act.

(d) the third party is not based in a country or jurisdiction assessed as high risk and

(e) the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures as applicable.

Salaried Employees:

In case of salaried employees, it is clarified that with a view to containing the risk of fraud, banks should rely on certificate / letter of identity/ address issued only from corporate and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate / letter. Further, in addition to the certificate / letter issued by the employer, banks should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN card, Voter's Identity card, etc.,) or utility bills for KYC purposes for opening bank accounts of salaried employees of corporate and other entities.

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, they 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.

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.

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. Branches 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. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. As mentioned under the Customer Acceptance Policy, accounts of such persons can be opened only with the permission of the respective Regional Office. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The aforesaid norms may also be applied to accounts of the family members or close relatives of the PEPs.

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly banks are opening accounts for customers without the need for 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 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. As mentioned under the Customer Acceptance Policy, accounts of non-face-to-face customers should be opened only with the permission of the respective Regional Office.

Walk-in-customers (non account based customers):

All transactions of walk-in customers pertaining to third party products are also subjected to KYC norms/AML measures as applicable to Banks products**.**

NOTE: In terms of Clause (b) (ii) of Sub-rule (1) of Rule 9 of the PML Rules, 2005, Branches are required to verify the identity of the customers for all International Money Transfer operations**.**

With regard to reporting of transactions carried out by walk-in-customers, detailed instructions are furnished under "Reporting of Cash/Suspicious Transactions" .

Accounts of Self Help Groups (SHGs)

KYC verification of all members of SHG need not be done while opening the SB account of the SHG and KYC verification of all the Office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, since KYC would have already been verified while opening the SB account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary.

Money transfer operations*.Multi Level Marketing (MLM) Agencies*

Reserve Bank of India have informed banks that certain firms posing as Multi Level Marketing (MLM) Agencies for consumer goods and services have been actually mobilising large amounts of deposits from the public with the promise of high returns. Eventually, such funds are used for illegal or highly risky purposes, putting the repayment of the deposits at risk. Hence, branches shall be extremely careful while opening accounts of MLM firms and ensure strict compliance with KYC/AML guidelines in such cases.

Hindu Undivided Family (HUF)

HUF comes into being because of a particular concept under Hindu Law whereby all the members of the family reside together jointly, carry on a business activity jointly and hold the property jointly and therefore, it is termed as Hindu Undivided Family.

The following documents are to be obtained for opening accounts of HUF:

Declaration from the Karta Proof of
Identification of Karta
Prescribed Joint Hindu Family Letter signed by all the adult coparceners.

Proprietary Concerns

As per RBI Master Circular dated 1.7.2014, Paragraph 2.5(h), the following are the list of documents that shall be provided as activity proof by the proprietary concerns:

1. Registration certificate (in the case of a registered concern),

2. Certificate/license issued by the Municipal Authorities under Shop & Establishment Act, Sales and Income Tax returns,

3. CST/VAT certificate,

4. Certificate/Registration document issued by Sales Tax/Service Tax/Professional Tax Authorities,

5. 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,

6. Registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department.

7. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT.

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

9. Utility bills such as electricity, water, and landline telephone bills in the name of the Proprietary Concern as required documents for opening of bank accounts of Proprietary Concerns

However, in cases where the Banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as mentioned above as activity proof. In such cases, the Banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the Proprietary Concern.

Operation of bank Accounts & Money mules

"Money Mules" are third-parties who are recruited by criminals who gain illegal access to deposit accounts, to launder the proceeds of fraud schemes (e.g. phishing and identity theft).

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. 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.

Branches are to strictly adhere to the guidelines (including RBI's Master circular) contained on KYC / AML/ CFT issued from time to time, periodically update the Customer Identification Data after the account is opened and also to monitor the transactions in order to protect themselves & customers from misuse by such fraudsters and to stop/ minimize operations of "Money Mules".

Accounts with introduction (Synd Samanya Account Product 221)

With a view to ensure that strict adherence to KYC Standards would not result in basic banking services being denied to underprivileged segments of the society (financial exclusion) the RBI has permitted flexibility in KYC Standards in opening of accounts for such persons to ensure that there is no financial exclusion.

The provisions for opening of bank accounts with restrictions on total credits and outstanding

balance, with introduction from an existing account holder or other evidence of identity and address to the satisfaction of the bank, were made to help persons who were not able to provide "officially valid documents" for opening accounts.

With the introduction of Accounts' and inclusion of the same in PML Rules, Accounts with introduction (called SyndSamanya SB A/c- Product 221 in our bank) stand withdrawn. However, Reserve Bank of India has introduced Basic Savings Bank Deposit Accounts in lieu of existing SyndSamanya SB accounts. Once Basic Savings Bank Deposit Accounts are introduced, existing SyndSamanya SB accounts will be converted as Basic Savings Bank Deposit Accounts.

Small Accounts

RBI, vide their circular No.RBI/2010-11/389 DBOD AML.No.77/14.01.001/2010-11 dated January 27, 2011, forwarded a Notification from Government of India, No.14/2010/ F.No.6/2/2007-E.S. dated December 16, 2010, amending 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.

The above Government Notification has introduced a new account category under Savings account called 'Small account''

A 'Small account' means a Savings account in a banking company where-

a) The aggregate of all credits in a financial year does not exceed rupees one lakh;

b) The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

c) The balanceat any point of time does not exceed rupees fifty thousand

The detailed procedure for opening 'Small accounts' are furnished hereunder.

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 -

1. the designated officer of the bank (Branch head or the next official in his absence), 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;
2. a Small account shall be opened only at Core Banking Solution linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to such accounts 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.
3. 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 bank 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

4. 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 as referred above and
5. 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 as mentioned above.

It is further advised that where a branch has relied exclusively on NREGA job card or Aadhaar letter for opening an account, it should be treated as Small account and shall be subject to all the conditions and limitations prescribed for Small account as above**.**

Difference between Small Account and Basic Savings Bank Account

A) For Small Accounts, RBI in its notification dated 26.08.2014 has mentioned that those persons who do not have any of the 'officially valid documents' can open "small accounts'' with banks.

B) Basic Savings Bank Deposit Account (BSBDA) would be subject to RBI instructions on Know Your Customers (KYC) / Anti Money Laundering (AML) for opening of bank accounts issued from time to time

It is evident from the above that BSBD Accounts are opened after complying with KYC/AML guidelines. It is therefore requested that those customers who have opened their BSBD Accounts are not asked to seek KYC documents again like customers of small accounts.

Definition of transactions:

Transaction means a purchase, sale, loan, pledge, gift, transfer, delivery or the agreement there of and includes-

Opening of an account;

- Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- The use of a safety deposit box or any other form of safe deposit;
- Entering into any fiduciary relationship;
- Any payment made or received in whole or in part of any contractual or other legal obligation;
- Any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and •

Establishing or creating a legal person or legal arrangement.

3. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures.

(a) Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose for the accounts where credit summations are more than Rs.1.00 lac per month. 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. These records are required to be preserved for five years as is required under PMLA,2002. Such records and related documents should be made available to help auditors in their

work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

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

(c) Customer profile as per **Annexure-3** and the record of transactions in the accounts are to be preserved and to be maintained in hard as well as soft copy as required in terms of section 12 of the PML Act, 2002, for a period of at least 5 years after the transaction has taken place and these records should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

(d) It will 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 through Principal Officer i.e. GM (Inspection). Some examples of suspicious activities/transactions to be monitored by the operating staff are given in **Annexure-IV**

(e) In case of an account already opened where a branch has not been able to apply appropriate KYC measures due to non-furnishing of information and/or non-co-operation by the customer, the branch should consider **blocking of further transactions /** closing the account or terminating the banking business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Further, decision in such cases should be taken by the branch head only, after taking into consideration all the relevant facts.

Purchase of foreign exchange from customers:

For purchase of foreign currency notes and/ or Travelers' cheques from customers for any amount less than '50,000/- [earlier USD 200], or its equivalent, photocopies of the identification document need not be obtained. However, full details of the identification document should be maintained.

For purchase of foreign currency notes and/ or Travellers'cheques from customers for any amount equal to or in excess of ' 50,000/-, or its equivalent, the documents, as mentioned at (F-Part-II) annexed to A.P. (DIR Series) Circular No. 17 {A.P. (FL/RL Series) Circular No.4} dated November 27, 2009, should be verified and copies retained.

In case of any suspicion of money laundering or terrorist financing, irrespective of the amount involved, enhanced Customer Due Diligence (CDD) should be applied.

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, post a low risk, APs should carry out full scale Customer Due Diligence (CDD) before undertaking any transaction for the customer.

Wire Transfers:

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 analyzing 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.

It must be ensured that all wire transfers are accompanied by the following information:

i) Cross-border wire transfers

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

(b) 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.

(c) 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 (b) above.

Guidelines on reporting of cross border wire transfers (CWTR) has been communicated vide RBI Circular no. DBOD.AML.NO.16415.714.01.001/2013-14 dated 28.03.2014 as:

Every reporting entity is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India. Such transactions may be furnished to Director,FIU-IND by 15th of the succeeding month. 'Transaction Based Reporting Format' (TRF) already developed by FIU-IND and being used for reporting Cash Transaction Reports (CTR) , Suspicious Transaction reports (STR) and Non Profit Organizations Transaction Reports (

NTRs) may be used for reporting the Cross Border Wire Transfers. The information may be furnished electronically in the FIN-Net module developed by FIU-IND.

The above guidelines dated 28.03.2014 shall continue

ii) Domestic Wire Transfers

(a) 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.

(b) If bank has reason to believe that a customer is intentionally structuring wire transfers 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.

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

iii) Exemptions

Inter-bank 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.

Care is to be exercised that-

(a) Implementation of the KYC guidelines should not result in denial of banking services (including opening of account) to the public, especially to those, who are financially or socially disadvantaged.

(b) The broad regulatory guidelines on customer acceptance policy envisage that persons with criminal background and/or having connections with terrorist organizations will not be accepted as account holders. It may be necessary to ensure that banking facilities are not denied for genuine purposes merely for the reason that criminal charges have been leveled against them or they have undergone some form of punishment in the past.

(c) Introduction of large number of accounts by a single introducer [either account holder or staff] to be accepted with caution.

(d) At the time of opening the account / during periodic updation, only "mandatory" information required for KYC purpose which the customer is obliged to give while opening an account should be obtained. Other "Optional" customer details/ additional information, if required may be obtained separately after the account is opened only with the explicit consent of the customer.

(e) In case of existing account holders, KYC procedures have to be completed, based on materiality and risk, if not already done.

(f) The information collected from the customer will be treated as confidential and not divulged externally for cross selling or any other purposes.

(g) For Debit card, Credit card, Internet Banking facilities and other new technology products, the KYC norms as applicable for the risk categorization of the customer will be followed for new accounts.

(h) **KYC requirements and periodical updation thereof form part of AML/CFT guidelines and are applicable to Asset side Customers also (i.e., Credit card, Housing Loan, Personal Loan, Agricultural and Industrial Loans etc.,)**

Tipping off:

An important element to the success of the AML process is that the customers should not be informed (i.e., tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the designated authority namely Financial Intelligence Unit, India (FIU-IND).

The branches can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the customer arouse suspicion. Branches should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

Where it is known or suspected that a suspicion report has already been made internally or externally, and it then becomes necessary to make further enquiries, care must be taken to ensure that the suspicion is not disclosed either to the client or to any other third party. Subject to internal procedures, such enquiries should normally/only be made as directed by the Principal Officer.

Combating Financing of Terrorism:

a) In terms of PMLA Rules, suspicious transactions should include ***inter alia*** transactions which give rise to a reasonable ground for suspicion that these may involve financing of the activities relating to terrorism.

b) As and when list of terrorists individuals/organizations issued by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India / Reserve Bank of India,

CO:Planning & Development Department will circulate the list among branches through a BC circular. Branches shall ensure that the list is kept updated at their end.

The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

(i) "Al-Qaida Sanctions List", which is maintained by the 1267 / 1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The Updated Al-Qaida SanctionsList is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

(ii) "1988 Sanctions List", which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/comm ittees/ 1988/list.shtm l.

It may be noted that both "Al-Qaida Sanctions List" and "1988 Sanctions List" are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

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 lists. Further, banks should scan all existing accounts **to** ensure that no account is held by or linked to any of the entities or individuals included in the list.

Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

In case, the particulars of any of their customers match with the particulars of any individual/entity included in the updated consolidated list, branches should immediately inform full particulars of the funds, financial assets or economic recourses or related services held in the form of bank accounts by such customers to the Principal Officer (General Manager, HO:Inspection Department) through their respective RO so as to enable the Principal Officer to report the matter to the Joint Secretary (IS.I), Ministry of Home Affairs at fax No.011-23092569 and also convey the same over telephone No.011-23092736, not later than 24 hours from the time of the branch finding out such a customer. The Principal Officer shall report the matter to the Joint Secretary (IS.I), Ministry of Home Affairs, UAPA Nodal Officer of RBI and FIU-IND as per instructions contained in Paragraph No.6 of Circular No.242-2009- BC dated 26-10-2009.

c) Branches shall take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions viz. Iran, Uzbekistan, Pakistan, Turkmenistan and Sao Tome and Principe, as identified in FATF Statement of February 25, 2009 circulated to branches through BC circulars issued from time to time and exercise due care while handling transactions connected with these countries.

Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move those funds between the jurisdictions.

There will be considerable overlap between the movement of terrorist funds and the laundering

of criminal assets: terrorist groups are known to have well - established links with organized criminal activity. However, there are two major differences between the use of terrorist and criminal funds-

Often only small amounts are required to commit a terrorist activity, thus increasing the difficulty of tracking the funds;

Terrorists can be funded from legitimately obtained income, including charitable donations, and it is not clear to a Branch at what stage legitimate earnings become terrorist assets.

Branches shall exercise caution if any transaction is detected in respect of terrorists/ terrorist organizations, lists of which are being circulated from time to time.

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

i) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 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. 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.

ii) Banks are required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex III) and ensure meticulous compliance to the Order issued by the Government/RBI from time to time.

Recognizing and Reporting Suspicious Transaction/Activity

What is meant by "suspicion"

The Rules notified under the PML Act, 2005 define a "suspicious Transaction" as a transaction whether or not made in cash which, to a person acting in good faith-

(a) Gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the schedule to the PML Act, 2005, regardless of the value involved.

(b) Appears to be made in circumstances of unusual or unjustified complexity; or

(c) Appears to have no economic rationale or bonafide purpose or

(d) 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.)

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion may be defined as being beyond mere speculation and based on some foundation i.e. "A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."

What is meant by reasonable grounds to suspect:

'Reasonable grounds to suspect' introduces an objective test rather than the subjective test of suspicion. It might therefore be defined in terms of 'wilful blindness'
i. e. turning a blind eye to the obvious; or negligence i.e. willfully and recklessly failing to make the adequate enquiries that an honest person would be expected to make in the circumstances; or failing to assess adequately the facts and information that are either presented or available and that would put an honest person on enquiry. Branch staff may need to be able to demonstrate that they took all reasonable steps as a person acting in good faith would take in the particular circumstance; to know the customer and the rationale for the transaction or the instruction. Branches should submit STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences of PMLA,2002.

An indicative list of Suspicious Activities is given in **Annexure-IV.**

Reporting of cash /Suspicious Transactions:

The provisions of the PML Act amendment Rule 2007 place an obligation on banks to furnish information in respect of suspicious transactions within seven working days from the date of occurrence of such transactions (on being satisfied that the transaction is suspicious) to the Director, Financial Intelligence Unit -India (FIU IND) in the prescribed format.
17
-All series of cash transaction integrally connected to each other which have been individually valued below Rs 10 lakh or its equivalent in Foreign Currency where such series of tyransaction have taken place within a month and the "month aggregate" exceeds Rs 10 lakh or its equivalent in foreign currency (Cir No 280/2014 page no 5) should also be reported to Financial Intelligence Unit -India (FIU-IND) by 15th of succeeding month in the prescribed format as given in circular No.105-2006-BC-P&D dated 19.05.2006. For determining integrally connected cash transactions, branches should take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month. However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated. Illustration of integrally connected cash transactions is shown in Annexure- V.A. CTR should contain only the transaction carried out by the branches on behalf of their client/customers excluding the transaction between internal accounts of the bank**.**

CBS branches may discontinue submission of Manual Cash Transaction Reports (CTR) with immediate effect, if not already done. CBS branches shall ensure that the CTR data generated by CO:DIT is downloaded by them monthly, verified, properly filed and stored. Further, the customer and accounts profile shall be updated into the system so that the CTR data filed with the FIU-IND is complete and accurate.

Cash transaction reporting by branches to their Principal Officer should invariably be submitted on monthly basis and the Principal Officer, in turn should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

The above transactions are to be reported by 15th day of succeeding month to FIU-IND, MOF, GOI. New Delhi. The delay as per Rule No. 8 in furnishing the information to the FIU-IND shall constitute a separate violation.

Branches shall maintain proper record of all transactions involving receipts by nonprofit organizations of value more than rupees ten lakh or its equivalent in foreign currency and till the reporting formats are circulated by RBI, Branches may report the transactions in the manual CTR formats prescribed for reporting Cash Transactions as per circulars issued in this regard.

However, the existing guidelines with regard to identification and reporting of suspicious transactions by all the branches should be scrupulously adhered to i.e., branches to report all suspicious transactions whether or not made in cash on the same day of arriving at a conclusion that the transaction is of suspicious nature to their RO in the prescribed format as given in circular No.105-2006-BC-P&D dated 19.05.2006. ROs shall forward STRs to HO:Inspection Department (KYC Cell) on the same day with their comments/remarks.

In respect of purchase of foreign exchange from customers, if the Authorised Person 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 A.P. should verify identity and address of the customer and also consider filing a suspicious transaction report to FIU-IND.

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. Further, if a Branch 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 address of the customer and also consider filing Suspicious Transaction Reports (STRs) immediately in appropriate cases, in the formats prescribed as per circular no. 170-2013-BC-P&D-40 dated 23.07.2013. Regional Offices should include suspicious transactions of non-account based customers, i.e. walk-in customers, in the quarterly reports on identification and reporting of suspicious transactions being submitted to Head Office:: Inspection Department.

In the new reporting format specifications, the banks are required to provide information about the source of alert and the alert indicator(s) for detection of suspicious transactions.

4. Risk Management

Bank’s internal audit and compliance functions have an important role in evaluating/ensuring adherence to the KYC policies and procedures.

RBI has advised the Banks to nominate a Designated Director for ensuring compliance with obligations under the PML Act as Circular No. DBOD.AML.BC.80/14.01.001/2013-14 dated 31.12.2013

Designation and address of the Designated Director is to be communicated to the Director, FIU-IND. It shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions referred to in rule 3.

The Banks are advised to adhere to the reporting requirement as per this new rule.

The Compliance Department of the Bank should provide an independent evaluation of the Bank’s own policies and procedures, including legal and regulatory requirements.

To ensure better execution of KYC / AML procedures and putting in place a sound monitoring mechanism in relation to the same, HO:Inspection Department is given the responsibility of handling the execution/monitoring aspects of KYC norms and AML measures including risk profiling of customers. The Department should ensure that their inspection machinery is staffed adequately with individuals who are well versed in KYC/AML policy 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.

5. Record Management

The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. REs shall,

(a) Maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;
(b) Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
(c) Make available the identification records and transaction data to the competent authorities upon request;
(d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) The nature of the transactions;
(ii) The amount of the transaction and the currency in which it was denominated;
(iii) The date on which the transaction was conducted; and
(iv) The parties to the transaction.
(f) 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; maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

As per RBI circular Ref. No. RBI/2010-11/532/ A.P. (DIR Series) Circular No. 62 dated 16.5.2011, for the following transactions, proper records are to be maintained as per Rule.3:

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 organizations of value more than Rupees ten lakh or its equivalent in foreign currency (Ref. Government of India Notification dated 12.11.2009- Rule 3, sub-clause (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.

Quoting of PAN

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

At-par cheque facility availed by co-operative banks

The 'at par' cheque facility offered by commercial banks to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising there from

Issuance of Prepaid Payment Instruments (PPIs):

PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment / hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML / CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML / CFT policies of the RE, regulation and related issues shall be ensured.

Branches shall be guided by the circulars issued by the Bank from time to time in this regard. Introduction of New Technologies - Credit Cards/Debit Cards/Smart Cards Branches 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. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers.

Applicability to Branches and subsidiaries outside India:

The above guidelines shall also apply to our London branch**.** In case local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank through International Division, Mumbai. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of Bank shall adopt the more stringent regulation of the two.

Principal Officer:

GM (Inspection) as the Principal Officer (Money Laundering Reporting Officer) 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 (CFT). The Principal Officer will be responsible for timely submission of CTRs, STRs and CCRs (reporting of counterfeit currency notes) to FIU-IND. **(Annexure V B,C,D)**

Employee Training:

Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML 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/AML policies and implement them consistently.

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.

Customer Education:

Implementation of KYC procedures requires Branches to demand certain information from customers which may be of personal nature or which has hitherto never been called for. The front desk staff shall be specially trained to handle such situations while dealing with customers.

Sharing of KYC documents in Fraud cases

Branches are to share the KYC documents with Paying / Collecting Banks (as the case may be) in respect of fraudulent transactions.

While sharing the copies of documents to facilitate paying Bank to lodge with the Police, the original documents shall be retained with the collecting Bank

Obligations of Payment System Operators under PML (Amendment) Act 2009:

RBI vide their circular No.RBI/2009-10/269.DPSS.CO.AD.No.1320/02.27.005/2009- 10 dated 02.12.2009 have advised all Payment System Operators authorized under the Payment & Settlement Systems Act, 2007 to put in place a proper policy framework on 'Know Your Customer', 'Anti-Money Laundering' and 'Combating of the Financing of Terrorism' measures with the approval of their Board. The list of authorized 'Payment System Operators' as on 31.1.2010 can be downloaded from RBI's website.

As per the above RBI circular all the Payment System Operators have been brought under the purview of PMLA, 2002 and all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency or all series of cash transactions integrally connected to each other which have been valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month, pertaining to the Authorised Person/Payment system operator have to be submitted in the form of Cash Transaction Report (CTR) to FIU-IND every month.

Similarly, all Payment System Operators have to report the following kinds of suspicious transactions, whether or not made in cash, to FIU-IND.

(a) Transaction which gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to have no economic rationale or bona fide purpose; or
(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

RBI has further advised that the guidelines contained in their above circular would also be applicable to all the agents and sub-agents of the Payment System Operators in India and it will be their sole responsibility to ensure that their agents and sub-agents also adhere to these guidelines.

Payment System includes the systems enabling Credit Card operations, Debit Card operations, Smart Card operations, Money transfer operations or similar operations. Departments making

use of the services of Payment System Operators shall from time to time ascertain from them that they have complied with the obligations of Payment System Operators under the PML (Amendment) Act, 2009.

Documents to be accepted while opening accounts in the case of following

Customer Due Diligence (CDD) Procedure

Bank shall obtain the following documents from an individual while establishing an account based relationship:

(a) One certified copy of an OVD containing details of identity and address;
(b) One recent photograph; and
(c) Such other documents pertaining to the nature of business or financial status. Provided that information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification under the PML Rules, as
(a) the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document', and
(b) Transfer of KYC data, electronically to the bank from UIDAI, is accepted as valid process for KYC verification.

CDD Measures for Sole Proprietary firms
For opening an account in the name of a sole proprietary firm, a certified copy of an OVD containing details of identity and address of the individual (proprietor) shall be obtained. In addition to the above, any two of the following documents as a proof of business / activity in the name of the proprietary firm shall also be obtained:

(a) Registration certificate
(b) Certificate / license issued by the municipal authorities under Shop and Establishment Act.
(c) Sales and income tax returns.
(d) CST / VAT certificate.
(e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
(f) Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities.
(h) Utility bills such as electricity, water, and landline telephone bills.
In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank may, at their discretion, accept only one of those documents as proof of business / activity.

For opening an account of a company, one certified copy of each of the following documents shall be obtained:
(a) Certificate of incorporation.
(b) Memorandum and Articles of Association.

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

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

For opening an account of a partnership firm, one certified copy of each of the following documents shall be obtained:

(a) Registration certificate.

(b) Partnership deed.

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

For opening an account of a trust, one certified copy of each of the following documents shall be obtained:

(a) Registration certificate.

(b) Trust deed.

(c) Officially valid documents in respect of the person holding a power of attorney to transact on its behalf.

For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the following documents shall be obtained:

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

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

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

(d) Such information as may be required by the Bank, to establish the legal existence of such an association or body of individuals

Procedure to be followed by banks while opening accounts of foreign students

(a) Banks shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

(b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA. 1999.

(c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.