KYC/AML/CFT POLICY

The Catholic Syrian Bank Ltd

PMLA Cell

Head Office Thrissur

PREFACE

The Prevention of Money Laundering Act, 2002 (PMLA) is enacted to prevent money laundering and to provide for confiscation of property derived from, or involved in, money laundering. The PML Act, and Rules notified there under, came into effect from 1st July, 2005. As per Section 3 of PMLA, "whosoever, directly or indirectly, attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of Money Laundering". The Act applies to the whole of India including Banks, Housing Finance Companies, Chit fund Companies, Intermediaries, Financial Institutions, NBFCs, Co-operative Banks & Money Changers.

Keeping in line with the Act this Revised KYC Policy book-let is a consolidation of the instructions on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

Reserve Bank of India [RBI] has advised banks to follow certain customer identification procedures while undertaking a transaction either by establishing an account based relationship or otherwise and monitor transactions of suspicious nature for the purpose of reporting it to appropriate authority.

These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). The FATF is an inter-governmental body formed by the G7 summit in Paris in the year 1989, whose purpose is the development and promotion of policies to combat money laundering and terrorist financing. FATF had advised all countries to set up ' Financial Intelligence Units' for collection of data on financial transactions and dissemination of these data to enforcement authorities for investigation. In line with this India has set up a Financial Intelligence Unit – India at New Delhi under the Ministry of Home Affairs. All banks and financial institutions are to report prescribed transactions on a regular basis to the FIU-IND.

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

These KYC/AML/CFT guidelines are issued under Section 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act mentioned elsewhere in this document and Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005.

Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act. It is pertinent to note that in the present context of terrorist activities and rampant black money, the Government of India and RBI are giving utmost importance to compliance of these guidelines and any lapse in this regard may result in substantial loss of reputation to the bank also

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

CONTENTS

1. Objective

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

2. Definition of Customer

For the purpose of KYC norms, a 'Customer' is defined as:

- a person who is engaged in a financial transaction or activity with the Bank
- and also includes a person on whose behalf the person who is engaged in the transaction or activity, is acting eg; Power of Attorney Holder, Beneficial Owner which means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law.

3. General

1. **Confidentiality of customer details**: Branch/Office 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. **Sharing of Information:** While considering the requests for data/information from Government and other agencies Branch/Office should exercise due diligence and shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
   The exceptions to the said rule shall be as under:
   i. Where there is a duty to the public to disclose,
   ii. the interest of bank requires disclosure and
   iii. Where the disclosure is made with the express or implied consent of the customer.

3. **Issue of DD/PO/MT/TT/NEFT/RTGS for Rs.50,000/- and above:** Branch/Office should ensure that any remittance of funds by way of demand draft/RTGS/NEFT, 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.

4. **Validity of Cheque/Draft/PO:** Branch/Office should not make payment of cheques/drafts/pay orders if they are presented beyond a period of three months from the date of such instrument.

5. **Adherence to Foreign Contribution (Regulation) Act, 1976:** Branch/Office should ensure that the provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable are strictly adhered to.

6. **Quoting of PAN:** Permanent Account Number of customers should be obtained & verified while undertaking transactions as per the provisions of the Income Tax Rule 114B applicable to banks including deposit in cash aggregating Rs 50,000/- or more with the bank during any one day, as amended from time to time. Form 60 should be obtained from persons who do not have PAN except for Private/Public Ltd Co & Partnership Firms who have to mandatorily submit PAN or proof of applying for PAN.

7. **Restriction in Collection of Account Payee Cheques:** Account payee cheques for any person other than the payee constituent shall not be collected. However, Branch/Office should at their option collect account payee cheques drawn for an amount not exceeding Rs.50,000/- to the account of their customers who are Co-operative Credit Societies, provided the payees of such cheques are the constituents of such Co-operative Credit Societies.

8. **Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standards (CRS):-** In 2010, the USA enacted FATCA with the objective of tackling tax evasion through obtaining information in respect of offshore financial accounts maintained by USA residents and citizens. The provisions of FATCA essentially provide for 30% withholding tax on US source payments made to Foreign Financial Institutions (FIs) unless they enter into an agreement with the Internal Revenue Service (IRS) to provide information about accounts held with them by USA persons or entities (firms/companies/trusts) controlled by USA persons. Since domestic laws of sovereign countries, (including India) may not permit sharing of client confidential information by FIs directly with USA, USA has entered into Inter-Governmental Agreement (IGA) with various countries. The IGA between India and USA was signed on 9th July, 2015, which provides that the Indian FIs will provide the necessary information to Indian tax authorities, which will then be transmitted to USA automatically. Under the IGA, USA will also provide substantial information about Indians having financial assets in USA.

   Similarly, to combat the problem of offshore tax evasion and avoidance and stashing of unaccounted money abroad requiring cooperation amongst tax authorities, the Group of Twenty Countries(G20) and Organization for Economic Cooperation and Development (OECD) countries working together developed a Common Reporting Standard (CRS) on Automatic Exchange of Information (AEOI). The CRS on AEOI was presented to G20 Leaders in Brisbane on 16th November, 2014. The CRS on AEOI requires the financial institutions of the “source” jurisdiction to collect and report information to their tax authorities about account holders “resident” in other countries, such information having to be transmitted “automatically’ on yearly basis. The information to be exchanged relates not only to individuals but also to shell companies and trusts having beneficial ownership or interest in the “resident” countries.

   In view of the commitment by Government of India to implement the CRS on AEOI and also the IGA with USA, and with a view to provide information to other countries, necessary legislative changes have been made through Finance (No. 2) Act, 2014, by amending section 285BA of the Income-tax Act, 1961. Income-tax Rules, 1962 were amended vide Notification

No. 62 of 2015 dated 7th August, 2015 by inserting Rules 114F to 114H and Form 61B to provide a legal basis for the Reporting Financial Institutions (RFIs) for maintaining and reporting information about the Reportable Accounts.

In this context of new global standards on Automatic Exchange of Information, under FATCA the Bank has to report details of US residents/citizens bank accounts identified on basis of certain 'Indicia', having balances above the threshold limit of U$ 50,000/- and under CRS the Bank has to report details of all Non-Residents other than US residents/citizens bank accounts

4. KYC Policy

The KYC Policy of the Bank is framed incorporating the following four key elements:

1. Customer Acceptance Policy;
2. Customer Identification Procedures;
3. Monitoring of Transactions; and
4. Risk Management.

4.1 Customer Acceptance Policy (CAP)

As per RBI guidelines, the bank has developed a Customer Acceptance Policy laying down explicit criteria for acceptance of customers including a description of the types of customers that are likely to pose a higher than average risk to the Bank. The CAP also enumerates explicit guidelines on the following aspects of customer relationship in the bank.

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

- Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. Branch/Office is unable to verify the identity and /or obtain documents required as per the risk categorization either due to non cooperation of the customer or non reliability of the data/information furnished to the bank by the customer. In case the Branch/Office identifies such accounts or comes across instances where the customer is reluctant to provide the required KYC documents/mandatory details under the policy, they should inform the PMLA Cell for further steps in this regard including closure of account after giving due notice to the customer explaining the reasons for such a decision.

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

- Before opening accounts in the name of PEPs (Politically Exposed Persons resident outside India)/relatives of PEPs, Branch/Office should obtain sanction from the Principal Officer for KYC/AML/CFT compliance.

- Branch/Office should not open current accounts of entities that enjoy credit facilities (fund based or non-fund based) from the banking system without obtaining a No-Objection Certificate (NOC) from the lending bank/s. Branches are permitted to open current accounts of such prospective customers in case no response is received from the lending bankers after a minimum waiting period of a fortnight. In case the prospective customer is a corporate or large borrower enjoying credit facilities from more than one bank, branches should exercise due diligence and inform the consortium leader if under consortium, and the lender banks concerned if under multiple banking arrangement. Branch/Office should not limit their due diligence to seeking NOC from the bank with whom the customer is supposed to be enjoying the credit facilities as per his/her declaration but also make use of the information available in the Central Repository of Information on Large Credits (CRILC) and verify whether the customer is availing of credit facility from other banks, from the data available in CRILC database. Branch/Office should also seek NOC from the drawee bank, if the initial deposit to the current account is by way of cheque.

  Branches should forward NOC or the letter addressed to the bank concerned after the period of 15 days, as the case may be, to CPC, along with other requisite documents for opening current accounts. CPC in turn should verify the documents received from branches with the details available in the CRILC, irrespective of the declaration obtained and submitted by the branches.CPC for this purpose is enabled to access the CRILC database. If the applicant is found to be enjoying credit facilities with other banks/FIs, CPC should direct the branch concerned, to obtain NOC from the identified bank/FIs as a precondition for opening the account. These instructions are aimed at enforcing credit discipline.

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

- To make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person whose name appears in the sanctions lists such as UNSCR, OFAC, E U Sanctions, H M Treasury's & Australian Autonomous Lists etc.; which is updated from time to time. In case of a positive match, the request to open the account should not be accepted and at the same time reported to the PMLA Cell for onward reporting to the FIU-IND. The Maarvel is designed to undertake such checks while opening accounts and during conduct of outward remittances of foreign exchange transactions. This exercise of updation of lists is being completed at the PMLA Cell. Further, the CBS should periodically scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the UNSCR list. Branch/Office is advised that full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to PMLA Cell, Head Office for onward reporting to RBI and FIU-IND.

- To also prevent opening of multiple client ID's in the names of existing customers through de-duping exercises.

- The Bank has a Board approved policy on Risk Categorization to effectively help in combating money laundering activities & terrorism given in Annexure I. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer

and his/her clients, mode of payments, volume of turnover, social and financial status, services availed etc. to enable risk categorization of customers into Low, Medium and High.

- Branch/Office is to prepare a profile for each new customer based on risk categorization as per the Board approved policy on risk categorization. The individual customer profile should contain mandatory information relating to customer's identity, Occupation, Sources of fund, Annual income. The Corporate customer profile should reflect mandatory information such as, nature of business activity, annual gross turnover and their location etc. Mandatory information such as dealings with other Banks including credit facilities should also be obtained from all customers. The nature and extent of extra due diligence should depend on the risk perceived by the Branch/ Office. However, while preparing customer profile Branch/Office should take care to seek only such information from the customer, which is relevant to the risk category and should not be intrusive. Optional/additional information should be obtained with the explicit consent of the customer after the account is opened. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes. The Bank has also put in place a system of periodical review of risk categorization of accounts. **Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months**.

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

The Bank should deploy 'Decoy Customers' to the branches so as to test the extent of compliance with KYC/AML norms the Branch/Office undertakes before commencing a business relationship with the customer. The Board has directed that the exercises should be conducted at quarterly intervals.

Customer Identification Procedure (CIP)

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

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

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

Person in terms of PML Act includes:
(i) an individual,
(ii) a Hindu undivided family,
(iii) a company,
(iv) a firm,
(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and
(vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

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

For customers that are **legal persons or entities**, the Branch/Office should

i. verify the legal status of the legal person/ entity through proper and relevant documents;

ii. verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person;

iii. understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution.

The Branch/Office should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied, that it knows who the beneficial owner(s) is/are. Procedures to determine the beneficial owner is given in Annexure II.

When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, Branch/Office should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

4.2.1 Unique Customer Identification Code

Under Unique Customer Identification Code (UCIC) a customer should have only one client ID in a Bank. UCIC, or allotting of a unique identification number to each customer, help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers including setting up of a ***Centralized KYC Registry***. The Bank has implemented UCIC while opening new accounts of fresh customers as well as for the existing customers. The Maarvel software is so designed that at the time of opening of accounts, the profile of the customer and the unique number of his/her KYC documents submitted is searched in the existing data base. In case of any positive identification by the Branch/Office, the account is opened under the existing allotted unique client/ Apex Client ID. ***Branche/ Office should open accounts of their customers under this unique client only.***

The Bank has a policy approved by the Board that clearly spells out that the Customer Identification Procedure is to be carried out at different stages i.e.

1. while establishing a account-based banking relationship;
2. as a part of KYC updation of an existing customer at periodic intervals under RBI guidelines, which is explained further on.
3. or when the Branch/Office bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
4. when the Branch/Office sells third party products as agents.`
5. while selling banks' own products, sale and reloading of prepaid cards and for any other product for more than Rs. 50,000/-.

6. when carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
7. when the Branch/Office has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

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

4.2.2 Customer Due Diligence measures while opening of accounts

Accounts of individuals:
While opening accounts in the name of individuals, Branch/Office should obtain one self attested copy of any one 'officially valid document' (OVD) as mentioned in Annexure III.A containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required.
A customer is required to submit only one OVD for both proof of identity and for proof of address (either current or permanent) as part of KYC procedure. If the OVD submitted for proof of identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

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

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

During account opening or while undergoing periodic KYC updation exercise where there is change of name due to marriage or any other circumstances Branch/Office should accept a true copy of marriage certificate issued by the Local Body/State Government in case of change in name due to marriage or Gazette notification indicating change in name in other cases, together with a certified copy of the 'officially valid document' in the existing name of the person.

Branch/Office is not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the bank to another branch. Branch/Office are advised that KYC verification once done by one branch of the bank should be valid for transfer of the account within the bank if full KYC verification has been done for the concerned account and is not due for periodic updation. KYC compliant customers should be allowed to transfer their accounts from one branch to another branch without restrictions, without insisting on fresh proof of address and/or identity and on the basis of a self-declaration from the account holder about his/her current address. Further, if an existing KYC compliant customer of the bank desires to open another account in the bank, there should be no need for submission of fresh proof of identity and/or address.

Since introduction is not mandatory for opening of accounts under PML Act and Rules/ Reserve Bank's extant instructions, Branch/Office should not insist on introduction for opening of bank accounts.

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

Simplified Measures for Proof of Identity for Low risk individuals:
If an individual customer does not have any of the OVDs (as mentioned in Annexure III.B) as proof of identity, then the Branch/Office is allowed to adopt 'Simplified Measures' in respect of 'Low risk' customers, taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category customers, where simplified measures are applied, it would be sufficient to obtain a certified copy of any one of the documents (as mentioned in Annexure III) which shall be deemed as an OVD for the purpose of proof of identity.

Simplified Measures for Proof of Address for Low risk individuals:
The additional documents (as mentioned in Annexure III.B) shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.
During the KYC updation or periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorized as 'medium' or 'high' risk category, then the Bank shall obtain one of the six OVDs listed in Annexure III.A of this Policy for proof of identity and proof of address immediately. In the event such a customer fails to submit such an OVD, Branch/Office shall initiate action as envisaged in 'KYC Non-Compliant Accounts - Freezing and closure of accounts' under 4.2.3 of. this Policy.

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

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

Small Accounts (BSBD)

If an individual customer, including a minor of the age of 10 years or above does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as mentioned in Annexure III.B), then 'Small Accounts' may be opened for such an individual. **Joint accounts, E or S accounts and accounts under guardianship are not permissible under this scheme.**

'Small account' means a savings account where:-

(i) The aggregate of all credits in a financial year does not exceed rupees one lakh;
(ii)The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
(iii) The balance at any point of time does not exceed rupees fifty thousand.

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

1. This account can be opened without any initial remittance, as there is no minimum balance stipulation for this account. The account shall carry no transaction costs or service charges/penalties whatsoever. Passbook facility shall be available for the account and the withdrawals shall be through withdrawal slip (spare cheque). However, **the passbook should not reflect address since it may be used as a KYC document in 'Low Risk Accounts'**. Instant Kit is not permitted to be issued for such accounts The following facilities, namely: cheque book, Debit/ATM cards, ABB facility and Internet Banking facility etc. that are normally available to KYC compliant accounts, shall not be available under BSBD Small account scheme. Foreign remittance should not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of "officially valid documents". These facilities shall be made available upon up gradation / conversion of a Small Account to a KYC compliant account after submission of valid KYC documents.

2. A 'small account' may be opened on the basis of a self-attested photograph and affixation of signature or thumb print. The officer of the branch, while opening the small account, should certify under his/her signature that the person opening the account has affixed his/her signature or thumb print, as the case may be, in his/her presence;

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 banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.
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; and
5. Alternatively, the account can be upgraded to a Regular Savings Bank Account, if so desired by the customer, in which case the Small Account has to be closed simultaneously.

6. If the customer fails to comply with the KYC norms within the maximum permitted relaxation period of 24 months from the date of account opening, the branch should freeze such small account/s under advice to the customer and no further credits/debits shall be allowed in such accounts

Third party verification of the identity of customers at the time of commencement of an account-based relationship

Branch/Office may rely on third party verifications of the KYC documents subject to the conditions that:-

- *the Branch/Office immediately obtains necessary information of such client due diligence carried out by the third party;*
- *the Branch/Office takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;*
- *the Branch/Office is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;*
- *the third party is not based in a country or jurisdiction assessed as high risk and*
- *the Branch/Office is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.*
- *In the case of NRI accounts the Indian Embassy of the respective country can be relied upon.*

Accounts of non-face-to-face customers

With the introduction of mobile phone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved.

Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, Branch/Office 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/Office 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 above.

Accounts of foreign students

Branch/Office should follow the following procedure for foreign students studying in India.

1. Branch/Office may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution in India.
2. Branch/Office should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.

3. During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.

4. The account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.

5. Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

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. Branch/Officeshould 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. Branch/Office should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.

The decision to open an account for a PEP will be taken by the Principal Officer for KYC/AML/CFT compliance which is clearly spelt out in the bank's Customer Acceptance Policy. Branch/Office should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, branch/office approval from the Principal Officer for KYC/AML/CFT compliance to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

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

Walk-in Customers

Walk-in Customer means a person who does not have an account based relationship with the Branch/Office, but undertakes financial transactions with the Branch/Office, eg; purchaser of DD/PO/NEFT etc,

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

However, if a Branch/Office has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the Branch/Office should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIUIND.

Note: The Bank is in terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 , is verifying the identity of the customers for all international money transfer operations. The Bank is also capturing the details of all walk-in customers in the Maarvel, including obtaining of KYC documents for identification purposes. Such walk-in customers are also being assigned walk-in-customer Client IDs.

Accounts of persons other than individuals:- Branch/Office should be vigilant against entities being used by individuals as a 'front' for maintaining accounts with banks. Branch/Office 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 including identifying the beneficial owner. 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.

Extra Due-Dilligence while opening Current Accounts

While opening Current Accounts the Bank has adopted the following extra due diligence measures:-

- Contact Point Verification (CPV) ie; the Branch Head or any other confirmed officer as directed by the Branch Head is to visit the place/office of the customer so as to collect such information as would be required to establish the existence of activity/business in the given address which is mandatory for all Current Accounts, except in the name of individuals. This should be certified in the Account Opening Form at the time of opening.

- For all walk in customers opening Current Accounts, the initial remittance should be taken by way of self cheque only and not cash. Exception is given to rural branches, where initial remittance can also be accepted in cash. Any exceptions to the above requires approval from AGM – CASA Vertical, HO. Walk in customers, in this context, are New to Bank customers without any reference. The 'walk in status' should be marked in the 'Account Opening Channel' field in the Account Opening Form.
- CRILC verification is made mandatory while opening Current Accounts.

Accounts of proprietary concerns:- Apart from the extant guidelines on personal identification procedure as applicable to the proprietor, Branch/Office should call for and verify the following documents before opening of accounts in the name of a proprietary concern that evidences name, address ,activity of the concern and the name of the proprietor, (In situations where the name of the proprietor is not available in the registration certificate/document, a self-attested true copy of the application for registration submitted by the applicant before the registering authority, wherein the name of the proprietor is stated, may be accepted as evidence of the name of the proprietor).

- Registration Certificate (in the case of a registered concern),
- Certificate/license issued by the Municipal authorities under Shop & Establishment Act,
- License/Certificate of Practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (d) CST/VAT certificate,
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
- Sales and income tax returns *(only as a second document)*
- 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 utility bills not more than 2 months old 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 *(only as a second document)*
- Though the default rule is that any two documents, mentioned above, should be provided as activity proof by a proprietary concern, in cases where the Branch/Office is satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the Branch/Office, 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. The branch official under official seal should evidence the same in the account opening form under the certification 'CPV undertaken & confirmed'. However, this is not applicable in cases where the activity proof document is mentioned as second document only.
- PAN Card in the name of the proprietor /firm or Form/60.

Accounts of Ltd / Pvt Ltd Company:- *O*ne certified copy each of the following documents are required for customer identification:

- Certificate of Incorporation & Memorandum & Articles of Association (to be verified with the original by the branch)
- A Resolution signed by the Company Secretary or the Authorized Signatory as per the Articles of Association, from the Board of Directors regarding opening of Bank Account, Authorized signatories, operation of account and power of attorney granted to its managers, officers or employees to transact on its behalf.
- Recent photograph & an officially valid document for ID & Address proof in respect of each Authorized signatories, managers or employees holding an attorney to transact on its behalf and that of Beneficial Owners, if any.
- Present list of Directors & their DIN Number.
- PAN Card or proof of applying for PAN

Accounts of registered Partnership firm:- One certified copy of the following documents is required for customer identification:

- Partnership Registration Certificate & Partnership deed (to be verified with the original by the branch)
- Resolution signed by all partners regarding opening of Bank Account & Authorized signatories, operation of account etc; if not specifically mentioned in the Deed.
- Recent photograph & an officially valid document for ID & address proof in respect of each of the Authorized Signatories & Beneficial Owners of the firm if any.
- If the deed is one of a reconstituted firm, the prior deeds if any and the original Partnership deed should be obtained & verified by the Branch
- PAN Card or proof of applying for PAN

Accounts of Trusts:- One certified copy of the following documents is required for customer identification:

- Trust Registration Certificate & Trust Deed. (to be verified with the original by the branch)
- Resolution signed by all trustees regarding opening of Bank Account & Authorized signatories, operation of account etc; if not specifically mentioned in the Trust Deed.

- Recent photograph & an officially valid document for ID and address proof in respect of the Authorized Signatories of the Trust/Foundation holding an attorney to transact on its behalf and that of Beneficial Owners of the Trust, if any.
- PAN Card or Form/60

Accounts of unregistered - Association / Body of individuals / Partnership Firm / Trust / Foundation:-One certified copy of the following documents is required for customer identification:

- Resolution of the meeting of the managing body of such association or body of individuals/Partnership/Trust/Foundation.
- Recent photograph & officially valid document for ID and address proof in respect of each Authorized Signatories / Partner / Trustee / Founder / Office bearers, managers including those, holding an attorney to transact on its behalf and that of Beneficial Owners, if any.
- Such information as may be required to the satisfaction of the Principal Officer of the branch to collectively establish the legal existence of such an association or body of individuals, Trust Deed in the case of Trusts and Partnership Deed in the case of Partnership Firms.
- PAN Card Form 60. For unregistered Partnership firms- PAN Card or proof of applying for PAN

Accounts of HUF's:-One certified copy of the following documents is required for customer identification:

- Letter of Joint Hindu Undivided Family in L-39, signed by the Kartha under official seal & other Major family members of the HUF
- Recent photograph and officially valid document for ID & Address proof in respect of the Kartha.
- PAN Card or Form 60

Simplified norms for Self Help Groups (SHGs)

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

Simplified KYC norms for Foreign Portfolio Investors (FPIs)

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

When the client accounts opened by professional intermediaries: When the branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branch may hold **'pooled' accounts** managed

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

A summary of the KYC documents that should be accepted for Individual & various Corporate categories at time of opening an account is listed in Annexure III for easy reference.

Periodic Updation of KYC

Branch/Office should introduce a system of periodical **update of customer identification data (including photograph/s)** even after the account is opened.

The periodicity of such KYC updation should not be less than :-

*once in **ten years** in case of **low risk** category customers,*
*once in **eight years** for **medium risk** category customers and …*
*once in **two years** in case of **high risk** category customers.*
The time limits prescribed above will apply from date of opening the account or last updation of KYC.

Such KYC exercise may include all measures for confirming the identity and address and other particulars of the customer that the Branch/Office may consider reasonable and necessary, based on the risk profile of the customer, taking into account whether and when client due diligence measures were last undertaken and the adequacy of data obtained. Fresh recent photographs should be obtained from customers including from minor customers who attain majority.

Branch/Office need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorized as 'low risk', in case there is no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Branch/Office should not insist on physical presence of such low risk customer at the time of periodic updation.

During the periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorised as 'moderate or ''high' risk category, then bank shall obtain one of the six OVDs listed at Section 3(a)(vi) of these Directions for proof of identity and proof of address immediately. In the event such a customer fails to submit such an OVD, Branch/Office shall initiate action as envisaged in the next paragraph **- KYC Non-Compliant Accounts - Freezing and closure of accounts**.

The said indicative list furnished in Annexure IV shall not be treated as an exhaustive list as a result of which KYC updation process may be hampered and the customer faces difficulties in transacting his/her business. Branch/Office should as far as possible rely on the OVD's as KYC documents while updating KYC in accounts.

KYC Non-Compliant Accounts - Freezing and closure of accounts

In case of non-compliance of KYC requirements by the customers despite repeated reminders by Branch/Office, Branch/Office may impose 'partial freezing' on such KYC non-compliant accounts in a phased manner. During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force. While imposing 'partial freezing', Branch/Office has to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirements to be followed by a reminder giving a further period of three months. Thereafter, Branch/Office may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts.

If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' the Bank should disallow all debits and credits from/to the accounts thereby, rendering them inoperative. The customers shall have the option to revive their account by submitting their KYC documents & individual profile form.

Further, it would always be open to the Branch/Office to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision

In the circumstances when a Branch/Office believes that it would no longer be satisfied about the true identity of the account holder, the Branch/Office will inform the PMLA Cell who in turn will file a Suspicious Transaction Report (STR) with Financial Intelligence Unit – India (FIU-IND) under Department of Revenue, Ministry of Finance, Government of India.

Closure of accounts

Where the Branch/Office is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking / business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken after confirmation from the Principal Officer for KYC/AML/CFT compliance.

4.3 Monitoring of Transactions

Transaction means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof 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; or establishing or creating a legal person or legal arrangement.

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

Branch/Office should pay special attention to all complex, unusually large transactions including RTGS transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Bank has prescribed threshold limits for different categories of accounts in its AML software and pay particular attention to the transactions which exceed these limits.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. Existing / newly opened accounts where deposit of third party cheques, drafts is made and followed by immediate cash withdrawals, especially through ATM's should be closely watched. Deposit of cash / cheques through different branches using ABB facility and withdrawals through ATM's that too in different locations are important indicators for suspected money laundering transactions.

Instances where DD's/PO's/NEFT's are purchased by Walk-in customers in cash, including structuring the amount to below Rs.50.000/- continuously in order to evade the limit of Rs 50,000/- set for issue of DD's/PO's/NEFT' in cash ,should be looked in to.

The transactions in accounts of marketing firms that appear as Multi-Level Marketing Firm, should be closely monitored for any suspicious activity. Branch/Office should subject accounts to enhanced monitoring where there is requisition for a large number of cheque books with multiple small deposits generally made in cash and large number of cheques are issued bearing similar amounts /dates.

Where such features are noticed and found suspicious, it should be brought to the attention of the PMLA Cell for onward reporting to the FIU-IND & RBI. The extent of monitoring should be aligned with the risk category of the customer.

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

Branch/Office should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his/her business and risk profile and where necessary, the source of funds.
Customers should neither be told nor given any room for doubts in their mind that while seeking additional information the Branch/Office is viewing at their transactions / activity with suspicion. Such disclosure / indication is against the provisions of relevant Act / guidelines.

Operation of bank accounts & Money Mules

"Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a

fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

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

Transaction Monitoring Processes

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

As pointed out above the Branch/Office should constantly keep a watch over the transactions conducted in accounts.

The PMLA Cell also constantly monitors all transactions in accounts with the support of AML software. Alerts are generated in the AML software based on specific scenarios & threshold limits based on the risk categorization of accounts. Suspicious transactions if any, after taking into account the views of the Branch/Office if required, are reported to the FIU-IND, New Delhi.

Transactions are also being monitored depending on the risk sensitivity of the account. Special attention is to be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

High risk accounts should be subjected to intensive monitoring. Suspicious Transactions Reports are to be filed with FIU-IND in respect of all suspicious transactions /activity finalized as such by the Principal Officer for KYC/AML/CFT compliance at Head Office.

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

Suspicious Transactions

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

- gives rise to a reasonable ground of suspicion that it may involve the **proceeds of crime**; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose;
- gives rise to a reasonable ground of suspicion related to identity of client such as;

    i. False identification documents
    ii. Identification documents which could not be verified within reasonable time
    iii. Accounts opened with names very close to other established business entities
    iv. Customer is reluctant to provide original KYC documents
    v. Is inconsistent while providing personal details

Background of client

- Suspicious background or links with known criminals
- Customer not located in the area where the account is opened

Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in accounts

- Unusual activity compared with past transactions
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business

Nature of transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Frequent purchases of drafts or other negotiable instruments with cash
- Nature of transactions inconsistent with what would be expected from declared business
- Unexplained Inward remittances
- High activity in form of credits by internal transfers/cash/clearing/RTGS followed by outward remittance
- Remittances through ABB, withdrawal through ATM's
- "U-Turn" Transactions i.e. money passes from one person or more than one persons but it finally returns to the hands of the original sender
- Routing of transfer through multiple locations

Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client's apparent financial standing

4.4 Risk Management

Branch/Office should exercise on going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds.

The Board of Directors of the bank is ensuring that effective KYC programme is put in place by establishing appropriate procedures and effective implementation. It also covers proper management oversight, systems and controls, segregation of duties, training of staff and other related matters.

In addition, the following is also ensured for effectively implementing the AML/CFT requirements

- Using a risk-based approach to address management and mitigation of various AML/CFT risks.
- Allocation of responsibility for effective implementation of policies and procedures.
- Independent evaluation by the compliance functions of the Banks policies and procedures, including legal and regulatory requirements.

  Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the Branch/Office and comment on the lapses observed in this regard. The PMLA Cell will also in turn follow-up with Branch/Office for timely rectification of the items pointed out.

- Putting up consolidated note on such audits to the Board through the Audit Committee at monthly & quarterly intervals.

Introduction of New Technologies – Credit cards/debit cards/ smart cards/gift cards
Branch/Office should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking and mobile banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

The bank is engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Branch/Office is required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Branch/Office is required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of all cardholders. Further, if agents are involved It is also desirable that agents are also subjected to KYC measures.

Correspondent Banking

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

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

Similarly, the bank should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/MD & CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval.

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

Correspondent relationship with a "Shell Bank"
The Bank does not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. The Bank should not enter into relationship with shell banks and before establishing correspondent relationship with any foreign

institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks.

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

Maintenance of records of transactions/Information to be preserved

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

Maintenance of records of transactions

The Bank should maintain proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

- all transactions reported in the Cash Transaction Report submitted to the FIU-IND monthly
- all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency
- 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
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Information to be preserved

Branch / Office is required to maintain all necessary information in respect of transactions referred to above to permit reconstruction of individual transaction, including the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction

Preservation of records

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

Branch/Office should ensure that records pertaining to the identification of the customer and his/her address obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request if required.

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

Branch/Office should maintain records of the identity of their clients, and records in respect of transactions related to STR/CTR/CCR/NTR/CBWTR in hard or soft format.

6. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

The PML Rules,2005 have been amended on 07/07/15 for setting up a Central KYC Record Registry. The Bank has been advised to be ready to share the KYC data of its clients with the CKYCR. The proposed CKYCR would receive, store, safeguard and retrieve the KYC documents of the client in digital form. The KYC records received from Banks and stored by the CKYCR could be retrieved online by any Bank across the financial sector for the purpose of establishing an account based relationship

7. Reporting Requirements

In terms of the PMLA Rules, the bank is required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than Rupees Ten lakh or its equivalent in foreign currency to the Director,Financial Intelligence Unit-India (FIU-IND) at the following address:

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

The Director, FIU-IND has powers to issue guidelines to Banks for detecting transactions referred to in various clauses of sub-rule (1) of rule 3 given above, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information. It is the duty of the Bank, Director, Officers and employees to observe the same.

The reporting formats and comprehensive reporting format guide, has been prescribed and released by FIU-IND including the Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation.

Cash Transaction Reports (CTR)

All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency; including 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 should be reported in the CTR. All accounts of the same customer should be taken into account while determining integrally connected transactions.

The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

A summary of cash transaction report for the bank as a whole should be generated at the PMLA Cell as per the format specified. The summary should be digitally signed by the Principal Officer for KYC/AML/CFT compliance and submitted to FIU-India.

Since the Bank's branches are under the Core Banking Solution (CBS) the Cash Transaction Reports (CTR) is generated at the PMLA Cell for onward transmission to FIU-IND.
The respective branches are instructed the identified cash transactions as stated above by PMLA Cell and are instructed to report any cash transactions of suspicious nature for onward reporting by the PMLA Cell to the FIU-IND under STRs.

Counterfeit Currency Report [CCR]

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

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

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer for KYC/AML/CFT compliance to FIU-IND in the specified format by 15th day of the next month .These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

The CCR is consolidated at the PMLA Cell based on the reports received from the designated Nodal branches / branch and the Currency Chest. Branch/Office is to report detection to the vigilance department in the specified format before the 5th of the succeeding month and also endorse a copy to PMLA Cell. The PMLA Cell in turn uploads the report in the prescribed format to the FIU-IND.

Suspicious Transaction Reports (STR)

The Bank is to furnish information to the FIU-IND regarding any suspicious transaction reported or detected during the course of its business.

Based on the recommendations of the IBA the Bank has notified the branches 27 offline scenarios which can be considered as suspicious and need to be reported to the PMLA Cell. These 27 offline scenarios are given in Annexure V. Branches should report suspicious transactions to PMLA Cell**,** if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction.

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

Similarly 43 scenarios have been recommended by the IBA for monitoring or recognizing unusual or suspicious transactions. The PMLA Cell constantly monitors all transactions in accounts with the support of the AML software 'Intellect' which is based on the scenarios given in Annexure V. Alerts are generated in the AML software based on specific scenarios & threshold limits.

Suspicious transaction with the investigation details or grounds of suspicion will be submitted to the Principal Officer for KYC/AML/CFT compliance for arriving at a conclusion. The Principal Officer for KYC/AML/CFT compliance should record his/her reasons for treating any transaction or a series of transactions as suspicious after taking into account the views of the Branch if required. Suspicious transactions if any, are reported to the FIU-IND, New Delhi under STR's. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office.
Information accompanying all domestic wire transfers including RTGS/NEFT 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. The beneficiary bank can return the wire transfers if such information is not available. When a credit or debit card is used to effect money transfer, necessary information as stated above should be included in the message.

If a Branch/Office has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Branch/Office 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.

The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. Such report should be made available to the competent authorities on request.

In the context of creating KYC/AML/CFT awareness among the staff and for generating alerts for suspicious transactions, Branch/Office shall consider the indicative list of suspicious activities pointed out in the Section 4.3 Monitoring of Transactions.

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

Non-Profit Organization Transaction Report (NTR)

Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO) as any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under section 25 of the Companies Act, 1956.

Branch/Office have to identify Non-profit Organization when opening accounts in the names of Trusts/Societies/Associations/Clubs/NGOs and mark the same in the Maarvel. The report of all transactions involving receipts by non- profit organizations of value more than Rupees Ten lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

Since all the branches of the bank are under the Core Banking Solution (CBS) the Non-profit organization's Transaction Reports (NTR) is generated at the PMLA Cell for onward transmission to FIU-IND.

Cross-border Wire Transfer (CBWTR)

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 fund from one location to another. 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 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.
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) 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.

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. Information accompanying all domestic wire transfers including RTGS/NEFT 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. The beneficiary bank can return the wire transfers if such information is not available.

d) 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.

Role of Ordering, Intermediary and Beneficiary banks

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.

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.

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.

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

All cross border wire transfers must be accompanied by accurate and meaningful originator information.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.

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 stated above.

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

Other General Guidelines

Section 51 A of the Unlawful Activities Prevention Act 1967

Section 51A reads as under:-

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

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

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

Freezing of financial assets

a) On receipt of the particulars as mentioned in paragraph 6(ii) above, IS-I Division of Ministry of Home Affairs(MHA) would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the branches are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by the bank is held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.
b) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the Unlawful Activities (Prevention) Act (UAPA) would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.
c) The order shall take place without prior notice to the designated individuals/entities.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/ entities inadvertently affected by the freezing mechanism

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

The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial

assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

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

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

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

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

9.Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) The bank is required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, the Bank should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. The Bank should also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

(b)The bank should examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

10.Powers of the FIU-IND

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

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

(2) If the Director, in the course of any inquiry, finds that a banking company, financial institution or an intermediary or any of its officers has failed to comply with the provisions contained in section 12, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may, by an order, levy a fine on such banking company or financial institution or intermediary which shall not be less than Rs. 10,000 but may extend to Rs. 100,000 for each failure."

11. Authority and Powers of the Directorate of Enforcement

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

- enter any premises of the bank/branch
- issues summons to the bank (all connected branches)
- conduct survey/inspection
- inspect & retain the records or the property
- check & verify any bank transaction
- call for information
- place identification marks
- make inventory
- record statements
- break open the lock, box, locker, safe, almirah
- seize any record or property or evidence
- examine any person on oath
- search any bank official
- arrest any person

12.Designated Director

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

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

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

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

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

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

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

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

The name, designation and address of the Designated Director is to be communicated to the Director, FIU-IND on any new appointment or change.
In addition it is the duty of the Designated Director to observe the procedures and manner of furnishing and reporting information on transactions related to STR/CTR/CCR/NTR/CBWTR.
It has been decided by the Board of Directors that the MD & CEO shall be designated as the Designated Director

13.Principal Officer of the Bank for KYC/ AML/ CFT compliance

The Bank should appoint a senior officer to be designated as Principal Officer for KYC/AML/CFT compliance. It should be ensured that the Principal Officer for KYC/AML/CFT compliance is able to act independently and report directly to the senior management. Principal Officer for KYC/AML/CFT compliance 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

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

The Principal Officer for KYC/AML/CFT compliance will also be responsible for timely submission of CTR/STR/CCR/NTR/CBWTR to FIU-IND.

With a view to enabling the Principal Officer for KYC/AML/CFT compliance to discharge his responsibilities effectively, the Principal Officer for KYC/AML/CFT compliance and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.The name, designation and address of the Principal Officer for KYC/AML/CFT is to be communicated to the Director, FIU-IND and the RBI on any new appointment or change.

It has been decided by the Board of Directors that the Head of the PMLA Cell will be designated as the Principal Officer for KYC/AML/CFT compliance and shall report to the Chief Compliance Officer.

14. Customer Education/Employee's Training/ Hiring of Employees

Customer Education

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

Employee's Training

The bank has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for

frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

Recruitment / Hiring of Employees

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

The importance of KYC norms to the employees

The employees of the bank will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff and management shall not provide advice or other assistance to individuals who are indulging in money laundering activities. Dereliction of duty and avoidance of knowledge on KYC / AML / CFT / obligation of bank will lead to examination / fixation of staff accountability.

Certain occasions arousing suspicion on bank employees:

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

15.<u>Duties/ Responsibility and Accountability of employees</u>

Personnel	Duties / Responsibilities
Officer in Charge of Accounts / Officer vested with authority to open new accounts /KYC Nodal Officer	1. To interview the potential customer 2. To verify the introductory reference / customer profile. 3. To arrive threshold limits for each account, new as well as existing, and to exercise due diligence in identifying suspicious transactions. 4. To prevent opening of accounts in the names of terrorist individual / entities / banned organizations 5. To adhere to the [provisions of Foreign Contribution Regulatory Act 1976, Prevention of Money laundering Act 2005, Unlawful Activities Prevention Act. 6. To comply with the guidelines issued by the Bank from time to time in respect of opening and conduct of accounts 7. To act as a liaison between the PMLA Cell

	and Branch/Office & see that the instructions issued by the PMLA Cell from time to time is complied with.
Principal Officer at branch/ office	1. To scrutinize and satisfy himself / herself that the information furnished in the account opening form / customer profile/ threshold limit/risk categorization are in strict compliance with KYC guidelines before authorizing / opening of account. 2. To certify in the Statement / Register regarding compliance with KYC guidelines and report all Suspicious Transactions and Counterfeit Currency Reports to appropriate authority in time.
Internal Inspectors / Concurrent Auditors / Inspecting Officials	To verify and report his/her comments on the effectiveness of measures taken by the Branch/Office and level of implementation of KYC/AML/CFT guidelines
Controlling Authority/Principal Officer for KYC/AML/CFT compliance	Prompt reporting of information regarding STR / CTR/CCR/CBWT/NTR to the law enforcing authority concerned in consultation with PMLA Cell, Head Office.

Evaluation of KYC Guidelines by Internal Audit and Inspection System

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

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

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

PMLA CELL [Prevention of Money Laundering Act Cell]

The Bank is fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. To address this the Bank put in place a PMLA Cell for addressing issues & obligations related to Know Your Customer/ Anti-Money Laundering / Combating Financing of Terrorism guidelines ie; The Prevention of Money-laundering Amendment Rules, 2009.

Activities of PMLA Cell

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

==========

ANNEXURE – I

Policy on Risk Categorization

This board approved policy on Risk Categorization which is a part of the Banks KYC policy effectively helps in combating money laundering activities & terrorism and also puts in place a system of periodical review of risk categorization of accounts which is to be conducted periodically not less than once in six months.

Bank has prepared a profile for each new customer based on risk categorization. Parameters of risk perception are clearly defined by undertaking customer due diligence measures in identifying the customer, the beneficial owner if any, verifying his/her identity by using reliable, independent source documents., data or mandatory information in terms of sources of funds, the nature of business activity, location of customer and his/her clients, mode of payments, annual turnover, social and financial status, services availed, credit facilities availed etc. available in the customer profile, to enable categorization of customers into Low, Medium and High Risk .

Branch/Office should obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship and thereby satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. For customers that are natural persons, the Branch / Office should obtain sufficient identification data to verify the identity of the customer, his/her address/location, and also his/her recent photograph. Bank should take steps to identify and assess their Money Laundering (ML) / Terrorist Financing (TF) risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels.

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

At the time of opening, the risk category of the account is based on the static parameters available in the profile form of the customer. Any later change in the profile / static data of the customer will also require re-categorization of the account. Re-categorization of the account will also be conducted at periodic intervals of six months as stated earlier, depending on the dynamic parameters such as velocity and volume of the transactions, the type of transactions and the status of the account.
The nature and extent of due diligence is based on the following principles:-

Low Risk Customers
Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. Further, Non-Profit Organizations (NPOs)/ Non-Government Organizations (NGOs) promoted by the United Nations or

its agencies, and such international/ multilateral organizations of repute, may also be classified as low risk customers.

Medium Risk Customers

Customers that are likely to pose a higher than average risk to the bank should be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his/her client profile, facilities or services enjoyed etc. Persons in business/industry or trading activity where the area of his/her residence or place of business has a scope or history of unlawful trading / business activity.

High Risk Customers

The branches may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. **Examples of customers requiring higher due diligence** include (a) Non-Resident customers; (b) High Networth Individuals (HNIs); (c) Trusts, Charitable Institutions , NGOs and Organizations receiving donations; (d) Companies having close family shareholding or beneficial ownership; (e) Firms with 'sleeping partners'; (f) Politically Exposed Persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; (g) Non-face to face customers and (h) those with dubious reputation as per public information available (i) Accounts of bullion dealers including sub-dealers and jewelers.

Characteristics of High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN1267 etc.
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities.
3. Individuals and entities in watch lists issued by Interpol and other similar International organizations
4. Customers with dubious reputation as per public information available or commercially available watch lists
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high risk
6. Customers conducting their business relationship or transactions in unusual circumstances such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
7. Politically exposed persons(PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
8. Non-resident customers and foreign nationals.
9. Embassies/Consulates
10. Off-shore (foreign) corporation/business
11. Non face-to-face customers
12. High net worth individuals
13. Firms with 'sleeping partners'
14. Companies having close family shareholding or beneficial ownership
15. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries where there is no legitimate commercial rationale

16. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
17. Investment Management / Money Management Company / Personal Investment Company
18. Trusts, charities, NGOs/NPOs
19. Money Service Business: including seller of : Money Orders/ Travelers' Checks/ Money Transmission/Check Cashing/ Currency Dealing or Exchange
20. Gambling/gaming including "Junket Operators" arranging gambling tours
21. Dealers in high value or precious goods(e.g. jewel, gem and precious metals dealers
22. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
23. Customers engaged in industries that might relate to nuclear proliferation activities or explosives
24. Customers that may appear to be Multi Level Marketing (MLM) companies etc.
25. Import/Export
26. Gas station
27. Car/Boat/Plane Dealership
28. Used car sales
29. Telemarketers

Characteristics of Medium Risk Customers

1. Non-Banking Financial Institution
2. Stock brokerage
3. Electronics(wholesale)
4. Travel agency
5. Providers of telecommunications service, internet café, IDD call service, phone cards,
6. Phone center
7. Dot-com company or internet business
8. Pawnshops
9. Auctioneers
10. Cash –Intensive Businesses such as restaurants, retail shops, parking garages, fast
11. Food stores, movie theaters, etc.
12. Sole Practitioners or Law Firms (small, little known)
13. Notaries
14. Secretarial Firms
15. Accountants
16. Venture capital companies
17. Account holders that enjoy services like Mobile Banking/ Internet Banking/ Anywhere Banking

Characteristics of Low Risk Customers

1. Economically backward people
2. Salaried Class
3. Students
4. Government Department/Organizations
5. Low turnover small balance accounts

Indicative list of High/ Medium risk products And Services

1. Internet Banking
2. Mobile banking
3. Trust and asset management services
4. Monetary instruments such as Travelers' Cheque

5. Trade finance
6. Anywhere banking services
7. Lending activities, particularly loans secured by cash collateral and marketable securities
8. Project financing of sensitive industries in high risk jurisdictions
9. Services offering cash, monetary or bearer instruments; cross-border transactions etc.
10. Non-deposit account services such as Non-deposit investment products and insurance

Indicative list of High/ Medium Risk Geographies

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

Locations

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

Risk Matrix for Re-categorization Purposes

The following points should be considered in the process of Risk Categorization:-

a) During account opening the final Risk Category of an account should be done on an averaging basis in the following manner. 40 % and above of the 10 parameters will determine the risk while taking into account the Static Parameters.ie; Sl: No: 1 to 10.

b) During re-categorization of risk every six months the Dynamic parameters will supersede the static parameters. (eg; If the account has been classified as 'Low Risk' by averaging the risk of static parameters & if any one dynamic parameter (except Turnover Type) is High, the account will be classified as 'High Risk')

c) Public Sector Co & Govt. Local Authority should always be categorized as Low Risk and all other corporate should fall under High or Medium Risk

d) The above rule will not be applicable to:-

- *Staff accounts (which will be always classified as low. Except when the quarterly average turnover exceeds Rs.3.00 lakh on re-categorization after the first six months)*

- *Student Support and Social Support Accounts (which will be always classified as low for the first six months and after that will depend on the dynamic parameters)*
- *NRI's should be always categorized as 'High Risk' for the first six months and after that will depend on the dynamic parameters.*
- *BSBD Small Account should be always categorized as 'High Risk'*

Individuals				Corporates		
Static Parameters				**Static Parameters**		
Parameters	**Risk Category**			**Risk Category**		
	High	**Medium**	**Low**	**High**	**Medium**	**Low**
Constituition	Individuals	Individuals	Individuals	Trusts,Charities, LLP, Sole Prop;Clubs,Association,Societies, Pvt / Ltd Co.	SHG,HUF	Public Sector Co,Govt Local Authority, Govt Organization only
Sources of Income	Business/Professional	Business/Professional	No income Daily wages Salaried/ Pension Agriculture Others	Foreign Exchange Business Banking / Manufacture Service, Trade Agriculture	Others	
Annual Income / Gross Turnover	Above 5 lakhs	> 1 lakh- 2.5 Lakh > 2.5 - 5 Lakh	<=1 Lakh	Above 25 lakh	upto to 25 lakh	
Product	Small Account, NRE/NRO Demand Deposits, Un Secured Loans, High Value Secured Loans above 20 lakh, Term Deposits > 25 lakh	Demand Deposits, Secured Loans <= 20 Lakh, Term Deposits 5 lakh to 25 lakh	Demand Deposits, Term Deposits < 5 lakh	Corporate / Un Secured Loans	Secured Loans,Demand Deposits, Term Deposits	
Services	Internet/Mobile Banking	Internet/Mobile Banking	Locker, ATM	Internet/Mobile Banking	Internet/Mobile Banking	
Location	**India**-Costal / Border / Criminal / Terrorist Outfit Bases/centers of High Risk Business/Others Abr**oad-** Non-FATF Members/UN Sanctions/Tax Havens/ Terrorism / Crime Bases /Others	Other areas	Other areas	**India**-Costal / Border / Criminal / Terrorist Outfit Bases/centers of High Risk Business/Others Abr**oad-** Non-FATF Members/UN Sanctions/Tax Havens/ Terrorism / Crime Bases /Others	Other areas	
Customer Category	NRI Politicians & relatives HNI	Businessman	Student Staff Salaried/Pensioner	NPO/PO Medium & Large Scale Industries Credit Societies/ Co operative Societies	SME, Banks Traders SSI Units	
Delivery Channel	Online	Walk-In Customers/Introduced By staff Marketing Team/Introduced By Others		Online	Walk-In Customers/Introduced By staff Marketing Team/Introduced By Others	
Mode of Operation	Minor / POA Holder	Representative Capacity	Single Joint Any One	Management Staff	POA Resolution/Single	
Nature Of Business/ Line Of Activity	NIL			Banking & Finance, Gold/ Cash Intensive Business Bullion/Import/Export Real Estate/ Construction	Others Agriculture	
Dynamic Parameters						
Monthly Turnover-Volume	> 1 lakh	0.25- 1 lakh	< 0.25 lakh	> 10 Lakh	1 lakh - 10 Lakh	<1 lakh
Monthly Turnover-	> 30 No's	10-30 No's	< 10 No's	> 50 No's	20-50 No's	< 20 No's

Velocity						
Turnover Type	Cash	Mixed	Mixed	Cash	Mixed	Transfer
Account Status	Inoperative/ STR / CTR / Frozen / Attached / Commented		Operative	Inoperative/ STR / CTR / Frozen / Attached / Commented		Operative

ANNEXURE – II

Procedure for Determination of Beneficial Ownership

While opening accounts in the names of Companies / Partnership Firms / Trusts/ Foundations, Associations/ Body of Individuals, Branch/Office should go through the Memorandum & Articles of Association/Partnership Deed / Trust Deed / Bye Laws not only to be aware of the legal & operational aspects of the entity but also understand the ownership & control structure so as to determine who are the natural persons that control the legal entity ie; the beneficial owner of the entity.

Under Rule 9(1A) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his/her identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person ie; an entity. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:

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

Explanation - For the purpose of this sub clause -

'Controlling ownership interest' means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;

'Control' shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements; Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management and where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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

c) **Where the client is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

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

e) **Where the client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust ie; the settler, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, branch/office should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branch/office should insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

ANNEXURE – III

A. Opening of Accounts -List of Officially Valid Documents (OVD's) to be obtained- Individuals

IDENTITY PROOF	ADDRESS PROOF
Valid Passport	Valid Passport
Valid Driving license	Valid Driving license
Voter's Identity Card issued by Election Commission of India,	Voter's Identity Card issued by Election Commission of India, (subject to address being cited in full)
Job card issued by NREGA duly signed by an officer of the State Government,	Job card issued by NREGA duly signed by an officer of the State Government
Letter issued by the Unique Identification Authority of India containing details of name,address and Aadhaar number (Aadhaar Card).	Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. (Aadhaar Card).
Permanent Account Number (PAN) Card	
In case the proof of address furnished by the customer is neither the local address nor the address where the customer is currently residing, the Branch / Office should take a declaration from the customer of her/his local address on which all correspondence will be made by the Branch / Office with the customer. No proof is required to be submitted by the customer for such address. This address, however, should be verified by the bank through 'Positive Confirmation' such as acknowledgment of receipt of letter cheque books, ATM cards etc;.	
As per Income Tax rules, quoting of Permanent Account Number (PAN) has been made mandatory for individuals, while opening a bank account (other than a basic savings bank deposit account) / a time deposit exceeding fifty thousand rupees (Rs.50,000/-) / aggregating to more than five lakhs rupees during a financial year / applying for a credit or debit card (other than Non-Residents). If a person does not have a Permanent Account Number and he enters into any transaction specified above, he/she shall make a declaration in Form No. 60 giving therein the particulars of such transaction, on each occasion the specified transactions are entered into.	

B. Other than the above further relaxations in the case of accounts of individual/s when categorized as 'Low Risk' has been allowed.

For ID Proof:-

a) Identity card with the applicants' **photograph** issued by Central/State Government Departments, Statutory / Regulatory Authorities, Public Sector undertakings, Scheduled Commercial Banks & Public Financial Institutions ***or…***

b) A letter issued by Gazetted Officer with a duly attested **photograph** of the person

For limited purpose of address:-

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

b) Recent Property or Municipal Tax Receipt;

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

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

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

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

g) Identity card with the applicants' **address** issued by Central/State Government Departments, Statutory / Regulatory Authorities, Public Sector undertakings, Scheduled Commercial Banks & Public Financial Institutions ***or…***

h) A letter issued by Gazetted Officer with a duly attested **address** of the person

Additional documents mentioned above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

C. Opening of Accounts -List of Officially Valid Documents (OVD's) to be obtained- Corporate Accounts

Accounts of Ltd / Pvt Ltd Company, one certified copy each of the following documents are required for customer identification: • Certificate of Incorporation & Memorandum & Articles of Association (to be verified with the original by the branch) • A Resolution signed by the Company Secretary or the Authorized Signatory as per the Articles of Association, from the Board of Directors regarding opening of Bank Account, Authorized signatories, operation of account and power of attorney granted to its managers, officers or employees to transact on its behalf. • Recent photograph & an officially valid document for ID & Address proof in respect of each Authorized signatories, managers or employees holding an attorney to transact on its behalf and that of Beneficial Owners, if any. • PAN Card or proof of applying for a PAN card. • Present list of Directors & their DIN Number
Accounts of registered Partnership firm, one certified copy of the following documents is required for customer identification: • Partnership Registration Certificate & Partnership deed (to be verified with the original by the branch) • Resolution signed by all partners regarding opening of Bank Account & Authorized signatories, operation of account etc; if not specifically mentioned in the Deed. • Recent photograph & an officially valid document for ID & address proof in respect of each of the Authorized Signatories & Beneficial Owners of the firm if any. • If the deed is one of a reconstituted firm, the prior deeds if any and the original Partnership

deed should be obtained & verified by the Branch
- PAN Card or proof of applying for a PAN card.

- Accounts of Trusts, one certified copy of the following documents is required for customer identification:
- Trust Registration Certificate & Trust Deed. (to be verified with the original by the branch)
- Resolution signed by all trustees regarding opening of Bank Account & Authorized signatories, operation of account etc; if not specifically mentioned in the Trust Deed.
- Recent photograph & an officially valid document for ID and address proof in respect of the Authorized Signatories of the Trust/Foundation holding an attorney to transact on its behalf and that of Beneficial Owners of the Trust, if any.
- PAN Card or Form 60

Accounts of unregistered - Association / Body of individuals / Partnership Firm Trust / Foundation, one certified copy of the following documents is required for customer identification:

- Resolution of the meeting of the managing body of such association or body of individuals/Partnership
- Trust/Foundation.
- Recent photograph & officially valid document for ID and address proof in respect of each Authorized Signatories / Partner / Trustee / Founder / Office bearers, managers including those, holding an attorney to transact on its behalf and that of Beneficial Owners, if any.
- Such information as may be required to the satisfaction of the Principal Officer of the branch to collectively establish the legal existence of such an association or body of individuals, Trust Deed in the case of Trusts and Partnership Deed in the case of Partnership Firms.
- PAN Card or Form 60

Accounts of Proprietary concerns:

For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern that evidences the name, address, activity of the concern and the name of the proprietor are required to be submitted: (In situations where the name of the proprietor is not available in the
registration certificate/document, a self-attested true copy of the application for registration submitted by the applicant before the registering authority, wherein the name of the proprietor is stated, may be accepted as evidence of the name of the proprietor.

(a) Registration certificate

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

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

(d) CST/VAT certificate.

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

(f) Sales and income tax returns (Only as a second document)

(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. (Only as a second document)

(h) Utility bills such as electricity, water, and landline telephone bills. (Only as a second document)

The above list is only illustrative and therefore includes license/certificate issued in the name of the proprietary concern by any professional body incorporated under a statute as one of the documents to prove the activity of the proprietary concern.

Though the default rule is that any two documents, mentioned above, should be provided as activity proof by a proprietary concern, in cases where the Branch / Office is satisfied that it is not possible to

furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the Branch / Office, 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. The branch official under official seal should evidence the same in the account opening form under the certification 'CPV undertaken & confirmed'. • PAN Card or Form 60
Accounts of HUF's, one certified copy of the following documents is required for customer identification: • Letter of Joint Hindu Undivided Family in L-39, signed by the Kartha under official seal & other Major family members of the HUF • Recent photograph and officially valid document for ID & Address proof in respect of the Kartha • PAN Card in the name of the HUF or Form 60
As per Income Tax rules, quoting of Permanent Account Number (PAN) has been made mandatory while opening a bank account in the names of Companies & Partnership firms. If any person, other than Companies & Partnership firms, does not have a Permanent Account Number and enters into any transaction specified above, they shall make a declaration in Form No. 60 giving therein the particulars of such transaction, on each occasion the specified transactions are entered into.

ANNEXURE – IV

Periodic Updation of KYC- Indicative list of documents to be obtained in existing client - Individuals

IDENTITY PROOF	ADDRESS PROOF
1.Aadhaar Card * 2.Passport* 3.Driving License* 4.Electoral ID Card 5.Letter from recognized public authority or public servant verifying the identity & residence of the customer* 6.Ration Card (subject to individual photograph of customer being affixed on the card) 7.PAN Card 8.Identity Card (issued by reputed employers-subject to the satisfaction of the Bank) 9. Job card issued by NREGA duly signed by an officer of the State Government	1.Aadhaar Card* 2.Passport* 3.Driving License* 4.Electoral Card (subject to address being cited in full)* 5.Letter from recognized public authority or public servant verifying the identity & residence of the customer* 6. Ration Card* 7.Domestic Gas consumer Card (Issued by PSU Co's) 8. Recent Telephone /Electricity bill 9.Bank Account Statement/Pass Book 10.Letter from employer (subject to the satisfaction of the Bank)
In case the proof of address furnished by the customer is neither the local address nor the address where the customer is currently residing, the Branch / Office should take a declaration from the customer of her/his local address on which all correspondence will be made by the Branch / Office with the customer. No proof is required to be submitted by the customer for such address. This address, however, should be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of letter cheque books, ATM cards etc;.	

For Periodic Updation of KYC in corporate accounts refer annexure III.C

ANNEXURE – V

IBA suggested Offline Alerts/Indicators for STR

Sl No	Alert Indicator Code	Alert Indicator
1	CV 1.1	Customer abandoned the transaction for the KYC requirement
2	CV 2.1	Customer offered false or forged identification documents
3	CV 2.2	Identity documents are not verifiable
4	CV 3.1	Address non-existent at the time of account opening
5	CV 3.2	Address found to be wrong at the time of account opening
6	CV 4.1	Complex structure created to avoid identification of beneficial owner
7	LQ 1.1	Customer is being investigated for criminal offences
8	LQ 2.1	Customer being investigated for select criminal offences
9	MR 1.1	Adverse media report for criminal activities
10	MR 2.1	Adverse media report about terrorist activities of customer
11	EL 1.1	Customer abandoned transaction when questioned
12	EL 2.1	Customer body language based alert
13	EL 2.2	Customer is over cautious
14	EL 2.3	Customer provides inconsistent information
15	EL 3.1	Customer appears to be acting on behalf while posting in person
16	EL 3.2	Multiple Customers working as a group
17	EL 4.1	Customer avoiding nearer branches without rationale
18	EL 4.2	Customer offers different identification on different occasions
19	EL 4.3	Customer purposely wants to avoid reporting
20	EL 4.4	Customer is not able to explain the source of funds
21	EL 5.1	Transaction is unnecessarily made to be complex
22	EL 5.2	Transaction has no economic rationale
23	EL 5.3	Transaction inconsistent with business/profile
24	EL 6.1	Unapproved inward remittances in NPO
25	PC 1.1	Complaints received from public
26	BA 1.1	Alerts raised by agent
27	BA 1.2	Alerts raised by other institution

IBA suggested Online Alerts/Indicators for STR generation

Sl No	Alert Indicator Code	Alert Indicator	Indicative Rule/Scenario
1	WL 1.1	Match with UN list	Match of customer details with individuals/entities on various UNSCR Lists
2	WL 1.2	Match with UAPA list	Match of customer details with designated individuals/entities under UAPA
3	WL 1.3	Match with other available lists	Match of customer details with TF suspects on lists of UNSCR, OFAC, E U Sanctions, H M Treasury's & Australian Autonomous Lists and other sources
4	WL 2.1	Match with other criminal list	Match of customer details with criminals on lists of Interpol, EU, OFAC, Commercial lists (World-Check, Factiva, LexisNexis, Dun & Bradstreet etc) and other sources
5	TM 2.1	High value cash deposits in a month	Cash deposits greater than INR[X1] for individuals and greater than INR[X2] for non individuals in a month Top[N] cash deposits in a month
6	TM 2.2	High value cash withdrawals in a month	Cash withdrawals s greater than INR[X1] for individuals and greater than INR[X2] for non individuals in a month Top[N] cash withdrawals in a month
7	TM 2.3	High value non-cash deposits in a month	Non- Cash deposits greater than INR[X1] for individuals and greater than INR[X2] for non individuals in a month Top[N] cash deposits in a month
8	TM 2.4	High value cash withdrawals in a month	Non- Cash withdrawals s greater than INR[X1] for individuals and greater than INR[X2] for non individuals in a month Top[N] cash withdrawals in a month
9	TM 3.1	Sudden high value transaction for the client	Value of transaction is more than [Z] percent of the previous largest transaction for the client (or client profile)
10	TM 3.2	Sudden increase in value of transactions in a month	Value of transactions in a month is more than [Z] percent of the average value for the client (or client profile)
11	TM 3.3	Sudden increase in number of transactions in a month	Number of transactions in a month is more than [Z] percent of the average number for the client
12	TM 4.1	High value transactions in the new account	Transactions greater than INR [X] in newly opened account within [Y] months
13	TM 4.2	High activity in a new account	Number of transactions more than [N] in newly opened account within [Y] months

14	TM 5.1	High value transactions in a dormant account	Transactions greater than INR[X] in dormant account within [Y] days of reactivation
15	TM 5.2	Sudden activity in a dormant account	Number of transactions more than [N] in dormant account within [Y] days of reactivation
16	TM 6.1	High value cash transactions inconsistent with profile	Cash transactions greater than INR [X] by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary person and Minor accounts
17	TM 6.2	High cash activity inconsistent with profile	Number of cash transactions greater than [X] by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and salary person and Minor accounts
18	TY 1.1	Splitting of cash deposits below INR 10 lac	Cash deposits in amounts ranging between INR 9,00,000/- to INR 9,99,999.99/- in multiple accounts of the customer greater than [N] times in a month
19	TY 1.2	Splitting of cash below INR 50000	Deposits of cash in the account in amounts ranging between INR 40000/- to INR 49999/- greater than [N] times in [Y] days
20	TY 1.5	Frequent low cash deposit	Cash deposits in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days
21	TY 1.6	Frequent low cash withdrawal	Cash withdrawals in amounts ranging between INR [X1] to [X2] greater than [N] times in [Y] days
22	TY 2.1	Many to one fund transfer	Funds sent by more than [N] remitters to one recipient
23	TY 2.2	One to many fund transfer	Funds sent by one remitter to by more than [N] recipients
24	TY 3.1	Customer trying to avoid linkage	Customer provided different IDs or Date of Birth at different instances
25	TY 3.2	Multiple customers working as a group	Common address/telephone used by multiple unrelated customers Common ID used by multiple customers Group of individuals conducting transactions
26	TY 5.1	Majority of card repayments in cash	Card repayments greater than INR [X] amount in cash in [Y] days ,Card repayment in cash is greater than [Z] percent of repayments in [Y] days
27	TY 5.2	Large credit balance in credit card	Debit balance in credit card is greater than INR[X]
28	TY 5.3	Large value card transactions for purchase of high value goods	Card usage greater than INR [X] for jewellery (MCC 5944) in [Y] days
29	TY 5.4	Large value cash withdrawals against international card	Cash withdrawals greater than INR [X] against international card in [Y] days
30	TY 5.5	Repeated small value cash withdrawals against international card	Cash withdrawals against international card in amounts ranging between INR[X1] to [X2] greater than [N] times in [Y] days in locations with known terrorist incidents
31	TY 5.6	Large repetitive card usage at the same merchant	More than [N] transactions at same merchant aggregating to more than INR[X] in [Y] days
32	TY 7.1	Repayment of loan in cash	Loan repayments in cash greater than INR [X] in [Y]

			months
33	TY 7.2	Premature closure of large FDR through PO/DD	Premature closure of FDR for amount greater than INR [X] within [N] days and payment by PO/DD
34	TY 7.3	High number of cheque leaves	Greater than [X1]number cheque leaves issued for savings bank account and [X2] number of cheque leaves issued for Current account in a period of [Y] days
35	TY 7.4	Frequent locker operations	Number of locker operations greater than [X] times in [Y] days
36	RM 1.1	High value transactions by high customers	Transactions greater than INR [X] by high risk customers (refer Appendix A)
37	RM 1.2	High value cash transactions in NPO	Cash transactions greater than INR[X] in Trust/NGO/NPO in [Y] days
38	RM 1.3	High value cash transactions related to real estate	Cash transactions greater than INR [X] related to real estate transactions in [Y] days
39	RM 1.4	High value cash transactions by dealer in precious metal/stone	Cash transactions greater than INR [X] by dealer in precious metal, precious stone or high value goods in [Y] days
40	RM 2.2	High value inward remittances	Inward remittance greater than [X] value aggregated in [Y] days
41	RM 2.3	Inward remittances in a new account	Inward remittance greater than [X] value in a new account within [Y] days
42	RM 2.4	Inward remittances inconsistent with client profile	Inward remittance greater than [X] value in [Y] days in account of Students, Housewife, Pensioners, Wages and Salary person and Minor accounts
43	RM 3.1	High value transactions with a country with high ML risk	Transaction greater than INR[X] involving a country considered to be high risk from the money laundering or drug trafficking perspective

****