# KNOW YOUR CUSTOMER STANDARDS

# AND

# ANTI MONEY LAUNDERING POLICY

## OF

**Version Number 1.10**
**Dated 31/05/2016**

**Document Update History:**

| Version No. | Date | Remarks | Created/updated by |
|---|---|---|---|
| 1.0 | | Initial Version For Approval of the Board | O&M&C |
| 1.1 | 10.09.2007 | Review and update | O&M&C |
| 1.2 | 16.06.2009 | Annual Review | O&M&C |
| 1.3 | 31.08.2010 | Annual Review | O&M&C |
| 1.4 | 27.09.2011 | Annual Review | O&M&C |
| 1.5 | 19.10.2012 | Annual Review | O&M&C |
| 1.6 | 19.04.2013 | Annual Review | O&M&C |
| 1.7 | 19.02.2014 | Annual Review | O&M&C |
| 1.8 | 06.04.2014 | Annual Review | O&M&C |
| 1.9 | 23.05.2015 | Annual Review | Compliance |
| 1.10 | | Annual Review | Compliance |

## 1. Preamble

1.1 In terms of the Guidelines issued by the Reserve Bank of India on Know Your Customer (KYC) norms, and Anti Money Laundering (AML) measures and combating of financing of Terrorism (CFT) obligations, Banks are required to put in place a comprehensive policy framework covering KYC norms, AML Measures and combating of financing of Terrorism (CFT) obligations.

1.2 The Know your customer guidelines issued by the Reserve Bank of India take into account the recommendations made by the Financial Action Task Force (FATF) on AML Standards and on combating financing of terrorism.

1.3 The guidelines also incorporate aspects covered in the Basel Committee document on customer due diligence which is a reflection of the International Financial Community's resolve to assist law enforcement authorities in combating financial crimes.

1.4 This policy document is prepared in line with the RBI guidelines and incorporate the Bank's approach to customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis.

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

## 2. Definition of Money Laundering

2.1 Section 3 of the Prevention of Money Laundering (PML) Amendment Act 2012 has defined the "Offence of money laundering" as under:

2.2 "Whosever directly or indirectly attempts to indulge or knowingly assists or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money laundering".

2.3 Money launderers use the banking system for cleansing 'dirty money' obtained from criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds.

2.4 For the purpose of this document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

## 3. Obligations under Prevention of Money Laundering [PML] Amendment act 2012.

3.1 Section 12 of PML Amendment Act 2012 places certain obligations on every banking company which include:

(i) Maintaining a record of all transactions, including information relating to transactions covered under (ii), in such a manner as to enable it to reconstruct individual transactions.

(ii) Furnishing to the Director (FIU) within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed.

(iii) Verifying the identity of its clients in such a manner and subject to such conditions, as may be prescribed.

(iv) Identifying the beneficial owner, if any, of such of its clients, as may be prescribed.

(v) Maintaining record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

(vi) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(vii) The recorded mentioned under (i) to (v) shall be maintained for a period of 5 years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

3.2 Section 12A of PML Amendment Act 2012 places certain obligations on every banking company which include:

(i) The Director may call for from any reporting entity any of the records referred to under Sec.12, and any additional information as he considers necessary for the purpose of the Act.

(ii) Every reporting entity shall furnish to the Director such information as may be required by him under Sec.12 within such time and in such manner as he may specify.

(iii) Save as otherwise provided under any law for the time being in force, every information sought by the Director under Sec.12 shall be kept confidential.

3.3 This policy document takes note of the obligations of the Bank under Sec.12 & Sec.12 A of the Prevention of Money Laundering Amendment Act, 2012, for strict compliance.

## 4. Money Laundering – Risk Perception

4.1 Money laundering activities expose the Bank to various risks such as:

4.2 **Reputation Risk:** Risk of loss due to severe impact on Bank's reputation. This may be of particular concern given the nature of the bank's business, which requires the confidence of depositors, creditors and the general market place.

4.3 **Compliance Risk**

Risk of loss due to failure of compliance with key regulations governing the bank's Operations.

4.4 **Operational Risk**

Risk of loss resulting from inadequate or failed internal processes, people and Systems or from external events.

4.5 **Legal Risk**

Risk of loss due to any legal action, the bank or its staff may face due to failure to comply with the law.

## 5. Policy Objectives

5.1 To prevent the bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

5.2 To enable the Bank to know/understand the customers and their financial dealings better, which in turn would help the Bank to manage risks Prudently.

5.3 To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

5.4 To comply with applicable laws and regulatory guidelines.

5.5 To take necessary steps to ensure that the concerned staff is adequately trained in KYC/AML procedures.

## 6. Scope

6.1 This policy is applicable to all branches and all other offices of the Bank and is to be read in conjunction with related operational guidelines issued from time to time.

**7. Definition of a Customer** 7.1 A Customer for the purpose of this policy is defined as:

(i) A person or an entity that maintains an account and/or has a Business relationship with the Bank.

(ii) One on whose behalf the account is maintained i.e. the beneficial owner

(iii) Beneficiaries of transactions conducted by professional Intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law and

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

7.1 General:

(i) 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 purpose. Bank will ensure that the information sought from the customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued. Bank will seek any other information from the customer separately, after opening the account and with the consent of the customer only.

(ii) Any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of traveller's cheque and Travel cards for value of Rupees fifty thousand and above will be effected by debit to the customer's account or against cheques and not against cash payment.

(iii) Bank will not make payment of cheques/drafts/banker's cheques, if they are presented beyond the period of three months from the date of such instrument, w.e.f 01/04/2012.

(iv) Bank will ensure that the provisions of Foreign Contribution Regulation Act, 2010, wherever applicable are strictly adhered to.

**8 . Key Elements of the Policy**

- Customer Acceptance Policy
- Customer Identification Procedures
- Monitoring of Transactions
- Risk Management

**8.1. Customer Acceptance Policy**

(i) Banks should prepare a profile for each new customer, by collecting duly filled up "KYC Data sheet" and the AML software application will do a risk categorization of each customer, using the various parameters of the customer profile as appearing in the KYC data sheet, which will be entered in the Core Banking application while creating the customer in the system.

(ii) The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc.

(iii) The Bank will take a risk based approach, so that the nature and extent of due diligence will depend on the risk perceived by the bank. A risk based approach means conducting the due diligence as per the perceived risk of the customer/potential customer. Thus in the case of a high risk category customer, the bank should conduct an enhanced due diligence, whereas in the case of a low risk customer, normal due diligence is sufficient.

(v) The bank will Classify the customers into various risk categories, based on the risk Perception and will decide on acceptance criteria for each category of customers:

(vi) The customers will be risk categorized as follows:

a. Very Low Risk

b. Low Risk

c. Medium Risk

d. High Risk

e. Very High Risk

(vii) Individuals (other than High Net worth Individuals) and entities whose identities and sources of wealth can be easily identified and transactions in whose account conform to the known profile will be classified as "Low Risk". For eg., salaried employees, People belonging to lower economic strata of the society, Govt. Departments, Govt. owned Companies, regulators, statutory bodies and NPOs/NGOs promoted by United Nations or its agencies.

(viii) Customers that are likely to pose a higher than average risk to the bank will be categorized as Medium or High Risk depending on the score of the customer for the parameters, as set up in the AML application like:

a. Gender

b. Income level

c. Occupation

d. Line of Business

e. Country of residence

f. Nationality

(ix) The following types of customers will be risk classified as "High Risk" or "Very High Risk".

a. Customers doing Cash intensive business like Bullion dealers, sub dealers and Jewellers.
b. Non- resident Customers
c. High Net worth Individuals
d. Trusts, Charities, NGOs and organizations receiving donations
e. Companies having close family holding or beneficial ownership
f. Firms with sleeping partners
g. Politically Exposed persons of foreign origin
h. Close relatives of PEP and accounts in which a PEP is the ultimate BO.
i. Non-face to face customers
j. Customers with dubious reputations

(x) A review of the risk categorization of the customers should be carried out at a periodicity of not less than once in six months. This will be done based the transaction history of the customer for the last six months on the following parameters:

a) Value of the cash and other transaction in the account, both debit and credit.

b) Velocity of the transactions in the account.

(xi) The Bank will accept customers after verifying their identity as laid down in Customer Identification Procedures detailed under Sec.8.2 of this Policy. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML

Amendment Act, 2010, and instructions/guidelines issued by Reserve Bank from time to time.

(xii) The Bank will not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. The decision by a branch to close an account in such cases should be taken by the Regional Office of the branch and the Branch shall close the account only after giving due notice to the customer explaining the reasons for such a decision.

(xiii) The Bank will not open accounts in the name of anonymous / fictitious / benami Persons/names:

(xiv) No transaction or account based relationship is undertaken without following the CDD procedure.

(xv) The Bank will do necessary checks before opening a new account, by way of a search of UN list of terrorists maintained in the AML software application and by way of a search in other public domain, if required, so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

(xvi) In occasions when an account is requested to be operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity, the Bank will enquire and ascertain the circumstances, in which a customer is permitted to act on behalf of another person/entity and will be clearly spelt out in conformity with the established law and practice of banking.

*(xvii)* Strive not to inconvenience the general public, especially those who are financially or socially disadvantaged. In order to avoid disproportionate cost to the banks and a burdensome regime for the customers, a risk based approach has been followed in the KYC Guidelines issued.

(xviii)While opening accounts of Politically Exposed Persons (PEPs) resident outside India, branches should obtain prior sanction from their respective Regional Offices.

(xix)The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

(xx) 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

(xxi) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(xxii) Bank will take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels, and to put in place controls and procedures, duly approved by the board, to effectively manage and mitigate the ML/TF risk, adopting a risk-based approach. Bank would thus adopt enhanced measures for products, services and customers with a medium or high risk rating. In this regard,

bank shall use for guidance in the risk assessment, the Report on **Parameters for Risk-Based Transaction Monitoring (RBTM) dated March 30, 2011 issued by Indian Banks' Association on May 18, 2011** as a supplement to their guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009.

**8.2. Customer Identification Procedures**

8.2.1 Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Branches 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.

8.2.2 Being satisfied means that the branch and the concerned officers 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.

8.2.3 Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.).

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

8.2.5 For customers that are legal persons or entities, the branches 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 the natural persons who ultimately control the legal person, viz., Beneficial Owner.

8.2.6 The Customer Identification Procedures are to be carried out at the following stages:

(i) While establishing a banking relationship ie an account based relationship

(ii) While carrying out a financial transaction

(iii) When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data

(iv) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

(v) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(vi) Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(vii) When a RE 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 rupees fifty thousand

(viii) While doing KYC updation- apply client due diligence measures to existing clients at an interval of two/eight/ten years in respect of high/medium/low risk clients respectively

While undertaking customer identification, REs shall ensure that :

8.2.7 Decision-making functions of determining compliance with KYC norms shall not be outsourced

8.2.8 Introduction shall not be sought while opening accounts

8.2.9 For determination of BO, the procedure advised by Government of India as communicated in RBI circular

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

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

8.2.12 It has been observed that some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account as the address in the Officially Valid Documents are different. In such cases, branches can obtain an OVD of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her.

Branches can also use any supplementary evidence such as a letter received through post for further verification of the address.

8.2.13 If an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise. KYC exercise once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account and the same is not due for periodic updation and a self-declaration from the account holder about his/her current address is obtained in such cases. The customer should be allowed to transfer his account from one branch to another branch without restrictions. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence

will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgement of receipt of (i) letter, cheque books, ATM cards (ii) telephonic conversation (iii)visits etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

8.2.14 Branches may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address, subject to verification by the bank through positive confirmation

8.2.15 Branches should intimate their customers that in the event of change in address due to relocation or any other reason, they should intimate the new address to the bank within two weeks of such a change. While opening new accounts and while periodically updating KYC data, an undertaking to this effect should be obtained. In case it is observed that the address mentioned as per 'proof of address' has undergone a change, REs shall ensure that fresh proof of address is obtained within a period of six months.

8.2.16 The customers shall not be required to furnish an additional Officially Valid Document(OVD), if the OVD submitted by the customer for KYC contains both proof of identity and proof of address. If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof of both identity and address. If the document submitted by you for proof of identity does not contain address details, then you will have to submit another officially valid document which contains address details. For identifying individual customers only one proof of address is required- either permanent or current address. If the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgement of receipt of (i) letter, cheque books, ATM cards (ii) telephonic conversation (iii)visits to the place etc.

8.2.17 Individuals who change their name due to marriage or otherwise, and the 'Officially Valid Document' (OVD) issued in the original name, which is not updated due to various reasons, still show the maiden/ previous name faced difficulties while opening new bank accounts or during periodic updation exercise or incorporating the name change in the existing accounts. As per the amendments, customers can submit a copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person even if there is change in the name subsequent to its issuance, while establishing an account based relationship or while undertaking periodic updation exercise or incorporating the name change in existing accounts.

8.2.18 As per the amendments in PMLA Rules 2013 banks should depend on documents which are identified as Officially Valid Documents for identifying individual customers and proof of address should follow from such Officially Valid Documents only. Later RBI had provided additional relaxations for the limited purpose of 'proof of address' in the case of low risk customers. In cases where the prospective 'low risk customers' are unable to produce any

Officially Valid Documents' for the proof of address, branches can accept the additional documents mentioned below without compromising on the customer identification guidelines.

- Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);
- Property or Municipal Tax receipt;
- Bank account or Post Office savings bank account statement;
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- 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
- Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

8.2.19 KYC PERIODIC UPDATION

Branches should introduce a system of periodical updation of customer identification data, by way of obtaining fresh customer identification documents, including photographs, after the account is opened. The periodicity of such updation should not be less than once in ten years in case of low risk category customers and not less than once in eight years in case of medium risk and two years in the case of High Risk categories. This periodical updation should be done by the Parent branch.

With a view to easing difficulties faced by common persons while opening bank accounts and during periodic updation, RBI simplified the KYC guidelines on periodic updation requirements. Branches need not seek fresh proofs of identity and address at the time of periodic updation, from 'low risk customers' in case of no change in status. A self certification by the customer to that effect should suffice in such cases. Branches do not insist on physical presence of the 'low risk' customers, in case of change of address they could merely forward a certified copy of the document (proof of address) by mail/post etc.

As regards non compliance of KYC requirements by the customers despite repeated reminders by branches, the branches should impose 'partial freezing' by allowing all credits and disallowing all debits on such KYC non-compliant in a phased manner. ie after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months.

8.2.*20* For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, banks, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

a) Necessary information of such customers' due diligence carried out by the third party is immediately obtained by bank.

b) Adequate steps are taken by banks to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be

made available from the third party upon request without delay.

c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

d) The third party shall not be based in a country or jurisdiction assessed as high risk.

e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.

8.2.21 **UCIC**

a. RBI advised that the increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers.

b. Banks were also advised to initiate steps for allotting UCIC to all their customers while entering into any new relationships for individual customers to begin with. UCIC should be allotted to all customers while entering into new relationships.

c. Branches should strictly follow the UCIC concept while creating new customers in the system.

d. The bank is committed to bring the legacy customers also under one customer ID.

8.2.22 **CDD Procedure in case of Individuals**

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

(a) one certified copy of an OVD as mentioned at Section 3(a)(vi) of Chapter I, containing details of identity and address;

(b) two recent photograph

Provided that information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

Explanation: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address.

8.2.23 An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in **Annex-I(a)** to this Policy. It is clarified that permanent correct address, as referred to in Annex-I, means the address at which a person usually resides and

can be taken as the address as mentioned in one of the officially Valid documents or any other document accepted by the bank for verification of the address of the customer.

8.2.24 The indicative list furnished in **Annex - I(a)**, is not an exhaustive list.

8.2.25 In respect of customers who are categorised as 'low risk' and are not able to produce any of the OVDs mentioned in Annex- I(a) and where 'simplified procedure' is applied, branches can accept any one document from each of the two additional sets of documents listed in Annex-I (b)

Explanation: During the periodic review, if the 'low risk' category customer for whom simplified procedure is applied, is re-categorized as 'moderate or ''high' risk category, then REs shall obtain one of the six OVDs listed at Annex I(a) of these Directions for proof of identity and proof of address immediately. In the event such a customer fails to submit such an OVD, REs shall initiate action as envisaged in Section 39 of these Directions.

8.2.25 **Customer identification requirements in respect of a few typical cases:**

**(i) Walk-in Customers**

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

Applicants for DD/MT/TT/Travelers cheques for amount exceeding Rs.10,000/- should record PAN Number on the application and copy of PAN card is obtained from the purchasers of such remittances.

If a branch has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the branch should verify the identity and address of the customer the customer's identity and address should be verified and copy of the Proof ID, Proof of Address and PAN should be kept with the transaction records.

If the suspicion is confirmed, the branch shall consider filing a suspicious transaction report (STR) to FIU-IND through Central AML Cell.

**(ii) Salaried Employees**

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

employees of corporate and other entities.

(iii) **Trust/Nominee or Fiduciary Accounts**

a. Trust/nominee or fiduciary accounts have the potential to misutilise to circumvent the customer identification procedures.
b. Branches should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branches should insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.
c. While opening an account for a trust, branches should take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.
d. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

(iv) **Accounts of Companies and Firms**

a. Branches need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with banks.

b. 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.

c. 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.

(v) **Client accounts opened by professional intermediaries**

a. When the branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified.
b. Branches 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.
c. 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, or where such funds are co-mingled at the level of bank, all the beneficial owners must be identified.
d. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.
e. Branches should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional

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

f. The ultimate responsibility for knowing the customer lies with the bank.

(vi) **Accounts of Politically Exposed Persons (PEPs) resident outside India**

a. Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

b. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

c. Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer.

d. Branches 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.

e. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, branches should obtain RO approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

f. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

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

(vii) **NRI Customers:**

The following customer identification documents should be obtained in the case of NRI customers:

**ID Proof:**

- Photocopy of all the pages of the Passport with stamping/entry containing Passport details and personal details for all the applicants.
- Copy of the valid Visa / Work Permit /Residence permit copy (either affixed in the passport or as a separate document).
- Two Passport size Photographs of each applicant.

**Address Proof**

The list of documents which can be accepted as address proof where the mailing address is an **overseas address** are as under:

- Photocopy of valid passport mentioning the overseas address;
- Photocopy of utility bill not more than 3 months old
- Photocopy of overseas bank statement not more than 3 months old
- Photocopy of valid driving licence
- Photocopy of the Government issued ID Card
- Photocopy of the credit card bill not more than 3 months old
- Photocopy of the lease agreement / rent receipt (not more than 3 months old.)
- Photocopy of the appointment letter
- Photocopy of the company ID Card with address
- Original Letter issued by the company for the purpose of account opening on itsletter head
- Photocopy of bank statement or passbook of a NRI Account with another bank
- Proof of address of the sponsor along with proof of relationship of the primaryapplicant with the sponsor
- Photocopy of the Overseas Citizen of India (OCI) Card mentioning the overseasaddress
- Photocopy of the Person of Indian Origin (PIO) Card mentioning the overseasaddress.

The list of documents which can be accepted as mailing address proof where the mailingaddress is an **Indian address** are as under

- Photocopy of Valid Passport;
- Photocopy of Valid permanent driving licence
- Photocopy of telephone bill of private and public operators not exceeding 2 months
- prior to the date of account opening
- Photocopy of electricity bill not exceeding 2 months prior to the date of account opening
- Photocopy of the Bank Pass Book or Bank Account Statement not exceeding 3
- months prior to the date of account opening
- Photocopy of the Ration Card
- Photocopy of the Election Card / Voters ID Card (if it has address)
- Photocopy of the title deeds of the property duly stamped and registered
- Photocopy of the Lease Deed / Rent Agreement Copy duly stamped
- Photocopy of the Senior Citizens Card from Indian Railways/Indian Airlines (if ithas address)
- Photocopy of the Mobile Phone post paid bill
- Letter from any recognized public authority (In original)
- Photocopy of Aadhaar Card

Persons settled overseas on a dependant visa need to provide proof of mailing address of the person sponsoring the dependant and proof of dependency / proof of relationship with theprimary applicant.

**Attestation of Documents and Personal appearance of the Customer:**

1. Personal appearance at the branches may be waived in the case of NRI customers, inview of the fact that they are residing abroad.

2. Since it is not possible for the NRI customer to produce the originals of the customer identification documents before the branch officials for verification and certification, hence the certification may be got done by embassy officials, KYC complied Bank abroad, KYC complied exchange house officials, Notary public, SIB officials deputed abroad etc. Alternatively, the documents may be self attested by the customer with full signature, provided additional documents as prescribed here below is furnished, in the case of Customer residing in an FATF country:

3. One document from any of the Additional Documents mentioned in List 1 and another from any of the additional documents mentioned in List 2, tabulated here below should be obtained.

**List 1**

1. An account payee cheque of existing NRE Account of the applicant with any Bank in India, drawn in his name for a minimum of Rs.2,000/-

2. An account payee cheque of existing domestic SB Account of the applicant with any Bank in India drawn in his name for a minimum of Rs.2,000/-; (If the customer submitting the domestic SB cheque, he must open an NRO Account also)

3. Original Account Statement of Overseas / Indian Bank Account at least for a period of 3 months period with the concerned bank's seal. (In case of online account statement it must be attested by bank officials.

**List 2**

1. A cheque drawn on a bank account abroad
2. Any cancelled paid cheque in photocopy drawn on a bank abroad showing the signature, bank name, account number etc
3. Photocopy Overseas / Indian Bank Statement not more than 3 months old
4. Photocopy Utility Bill (Overseas/Indian) not more than 3 months old
5. Photocopy of ID Card like valid permanent driver 's license, employee id card, labour card
6. Photocopy of local Government ID Card
7. Original Letter from the Employer issued for the purpose of opening this account
8. Photocopy of the Appointment Letter issued by the overseas employer for the employment overseas
9. Photocopy of the credit card statement not more than 3 months old
10. Photocopy of the lease / rental agreement / rent receipt (not more than 3 months old)
11. Photocopy of the Aadhaar Card.

**Customer residing in an Non-FATF country:**

All the photocopies of the Customer identification documents has to be attested by Indian Embassy or by a Notary.

**Quoting of PAN:**

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. If a PAN Card is available, photocopy of the PAN Card or Forwarding Letter of the PAN Card should be obtained.

Any person who does not have a permanent account number and who enters into any transaction in which quoting of PAN is mandatory, shall make a declaration in Form No. 60/61 as the case may be giving therein the particulars of such transaction. The Copy of Form No 60/61 so received shall sent the Jurisdictional Commissioner of Income Tax (Central Information Branch) on a half yearly basis.

If the minor/junior is not having income chargeable to tax, and has not yet obtained a PAN Card, the PAN of the Parent/guardian of the minor should be obtained. If the parent/guardian of the Minor is also not having PAN, Form No.60/61 signed by the Parent/guardian, with whose income the income of the minor is to be clubbed for Income Tax purpose, should be obtained. In that case the identification documents of the Parent/Guardian should also be obtained, as it is required to fill up Form No.60/61.

PAN Card should be insisted if the customer is opening an NRO Account, as the interest payable on the balance held in the NRO is subject to TDS, for remitting which to the Government; the PAN Card details are required. For availing the concessional TDS applicable to NRIs residing in countries having double taxation avoidance treaty with Govt. of India, NRI customer should provide a duly signed Form 10 F and also Tax residency certificate.

On a case to case basis branches are permitted to open NRO account with fully filled up and duly signed Form 60 along with a Self Declaration; in lieu of PAN while opening NRO accounts. However the branch should satisfy themselves that the NRI's income in India is not/ will not be exceeding the tax exemption limit prescribed under Income Tax rules.

The documents must be obtained annually besides obtaining at the time of opening account. The PAN continues to be mandatory for getting DTAA benefits and for proper remittance of TDS on NRO interest to government.

(viii) **Accounts of non-face-to-face customers**

a. The customer should visit the branch in person to create the customer/open the first account, along with the required customer identification documents, except in the case of NRI customers.
b. NRI customers are allowed to open the account through online mode, through the officers deputed to Hadi Exchange or by sending the required documents by post/courier.
c. The requirement of physical presence for creating the customer/opening the first

account for customer other than NRI customers may be waived by Regional Head, on request by the Branch with justification.

d. All the customer identification documents presented should be either presented in original or should be certified by the prescribed authority.
e. If the branch is relying on third party certification of customer identification documents, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.
f. The first payment to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face to face customers.

(ix) **Accounts of Proprietary concerns**

For opening an account in the name of a sole proprietary firm, a certified copy of an OVD as mentioned at Annexure 1(a) (vi), containing details of identity and address of the individual (proprietor) shall be obtained.

Apart from Customer identification procedure as applicable to the proprietor, branches should call for and verify any two of the documents listed in paragraph 2.5(h) of RBI master circular before opening of accounts in the name of a proprietary concern. However, in cases where branches are satisfied that it is not possible for the firm to furnish two documents as activity proof, they would have the discretion to accept only one of these KYC documents mentioned above is sufficient.

In such cases, branches would have to undertake contact point verification, collect such information as would be required to establish the existence of such a firm, confirm, clarify and satisfy itself that the business activity had been verified from the address of the proprietary concern.

The default rule is to obtain and verify any two of the following KYC documents (listed in paragraph 2.5(h) of RBI master circular) in the name of the firm before opening of accounts of a proprietary concern. The following list is only illustrative and therefore includes license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute, as one of the documents to prove the activity of the proprietary concern.

**Proof of the name**

- Address and activity of the concern like registration certificate (in the case of a registered concern)
- Certificate/ licence issued by the Municipal authorities under Shop & Establishment Act
- Sales and income tax returns
- CST/VAT certificate
- Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
- Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities,
- Registration/licensing document issued in the name of the proprietary concern by the Central

Government or State Government Authority/Department.

- IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT
- 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
- Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

However, in cases where banks are satisfied that it is not possible for the firm to furnish two documents as activity proof, they would have the discretion to accept only one of these KYC documents mentioned above is sufficient.

In such cases, banks would have to undertake contact point verification, collect such information as would be required to establish the existence of such a firm, confirm, clarify and satisfy itself that the business activity had been verified from the address of the proprietary concern.

X. **Small Accounts:**

In case an individual customer who does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at Annexure 1(a)& (b) and desires to open a bank account, banks shall open a 'Small Account', subject to the following:

(a) The bank shall obtain a self-attested photograph from the customer.

(b) The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

(d) Branches shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.

(e) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of "officially valid documents".

(f) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of "officially valid documents".

(g) The account remains operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.

(h) The entire relaxation provisions shall be reviewed after twenty four months.

- A Small account is one where all the following conditions are met:
    a. The aggregate of all credits in a financial year does not exceed Rs.1.00 lakh;

b. The aggregate of withdrawals and transfers in a month does not exceed Rs.10,000/-
c. The balance at any point of time does not exceed Rs.50,000/-.

- All the "Small accounts" in the Bank will be opened under the scheme "Basic Savings Bank Deposit Account"

- All the erstwhile "no frill accounts" - "Saral" also stands converted to the scheme "Basic Savings Bank Deposit Account" w.e.f 13/06/2013.

- In line with the RBI advice withdrawing the instructions for opening of accounts with introduction, the facility of opening accounts based on the "introduction from an existing customer" stands withdrawn.

XI. **Self Help Groups**

a. KYC verification of all the members of Self Help Group (SHG) need not be done while opening the savings bank account of the Self Help Group and KYC verification of all the office bearers would be sufficient.

b. As regards KYC verification at the time of credit linking of Self Help Groups (SHGs), it is clarified that since KYC would already have been verified while opening the savings bank account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary.

XII. **Operation of Bank Accounts & Money Mules**

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

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

c. The operations of such mule accounts can be minimised if branches strictly follow the guidelines on opening of accounts and monitoring of transactions.

XIII. **Bank No Longer Knows the True Identity**

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

**8.3. Monitoring of Transactions**

8.3.1 Monitoring of transactions will be conducted taking into consideration the risk profile of the account.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

8.3.2 A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

8.3.3 Branches have to take due care while opening accounts of Multi Level Marketing agencies to ensure that the firms are not being engaged in deposit taking activities and the funds raised by them are not being used for any illegal activities. Branches should closely monitor the transactions in accounts of marketing firms.

8.3.4 In cases where a large number of cheque books are sought by the company, and /or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, the branches should carefully analyse such data and in case they find such unusual operations in accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance.

8.3.5 Branches shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

8.3.6 Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored.

- Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or viable lawful purpose.
- Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose will be subjected to detailed scrutiny.
- Transactions which exceed the thresholds prescribed for specific categories of accounts.
- High account turnover inconsistent with the size of the balance maintained.
- Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

8.3.7 After due diligence at the appropriate level in the Bank, transactions of suspicious nature and/or any other type of transaction notified under PML Amendment Act, 2010 will be reported to FIU-IND through the Fin-net Gateway and a record of such transactions will be preserved and maintained for a period as prescribed in the Act.

8.3.8 A proper record of all transactions involving receipts by "Non-Profit Organizations (NPO's)", of value more than Rupees Ten Lakhs or its equivalent in foreign currency, should be extracted from the system and reported to FIU-IND through Fin-net gateway as NTR on a monthly basis.

8.3.9 "In the case of transactions carried out by a non-account based customer i.e. 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. Moreover, if the bank has reason to believe that the customer is intentionally structuring transactions into a series of transactions below the threshold limit of Rs.50,000/-,such cases should be reported to FIU IND as Suspicious Transaction Reports".

8.3.10 In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 branches and offices should verify the identity of the customers for all international money transfer operations.

8.3.11 Compliance of Provisions of Foreign Contribution Regulation Acts, 2010 should be ensured by the branches and offices, while allowing transactions involving donations and remittances from abroad.

### 8.4 Risk Management

8.4.1 The Board of Directors of the bank is responsible and committed to ensure that an effective KYC programme is put in place in the bank by establishing appropriate procedures and to ensure their effective implementation to achieve full compliance of KYC/AML/CFT guidelines of RBI in letter and spirit.

The Machinery for implementing the KYC Programme consists of:

**Board of Directors**

- Tasked with Formulating appropriate KYC/AML policies from time to time
- Direction and Advise on compliance of KYC/AML/CFT guidelines

**Audit Committee of the Board**

Tasked with

- the oversight of KYC/AML Compliance
- Review of KYC Inspection reports and status of rectification
- Identifying compliance threats

**Designated Director (MD&CEO)**

Board has approved Mr.V G Mathew, MD & CEO as the Designated Director for PMLA and stands duly communicated to FIU-IND. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include Oversight of implementation of the policies formulated by the Board Liaisoning with Director FIU-IND.

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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, 2013.

**AML Principal Officer (MLRO)**

- Monitoring the implementation of the bank's KYC/AML policy.
- Maintaining liaison with law enforcement agencies Ensuring submission of periodical Reports to the top Management/board.
- Oversight of timely submission of reports to FIU-IND viz., CTR, STR,CCR,NTR, Cross Border Wire transfers >5 lacs etc
- Formulation of Proper systems, procedures and Controls in the KYC/AML area
- Devise procedures for creating risk profiles of their existing and new customers
- Assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc
- Staff Training Programme on KYC/AML guidelines

**Central AML Cell**

- Transaction Monitoring through AML application
- Maintenance and development/customization of AML application in liaison with DICT and the system Vendor
- Timely submission of reports to FIU-IND Viz., CTR,STR,CCR,NTR, Cross Border Wire transfers >5 lacs etc.
- KYC/AML Inspection Reports
- Train the staff on KYC/AML guidelines

**Inspection & Vigilance Department**

Conducting Regular, Concurrent and Special KYC audits

**Regional Offices:**

- Oversight of compliance of KYC/AML guidelines by branches
- Following up and ensuring full rectification of deficiencies in KYC/AML compliance reported in various Inspections.

***Centralized Processing Centre***

The Bank **have implemented** Centralized Processing Center (CPC) Model for on boarding new customers in all regions.

**Compliance Function**

- Evaluating and ensuring adherence to the KYC policies and procedures (based on KYC
- Inspection reports, feedback from **CPC** etc) by the branches.
- Independent evaluation of the bank's own KYC/AML/CFT policies and procedures vis-à- vis legal and regulatory requirements

**9. Customer Education**

i. The Bank recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose.

ii. Bank will prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme.

iii. The front desk staff will be specially trained to handle such situations while dealing with customers.

**10. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.**

(i) Bank will pay special attention to the money laundering and financing of terrorism threats arising from new or developing technologies, including internet banking that might favor anonymity, and take necessary steps to prevent its misuse for money laundering activities.

(ii) It shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

(iii) We are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Branches have to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also.

(iv) Bank will ensure that appropriate KYC Procedures are duly applied to the customers using the new technology driven products.

(v) Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

**11. Combating Financing of Terrorism**

(i) In terms of PMLA Rules, suspicious transaction should include transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities

relating to terrorism. Branches are, therefore, advised to have ongoing, enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-IND through Central AML cell.

**(ii)** As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. AML central cell should ensure to update the lists of individuals and entities as circulated by Reserve Bank in the AML software application**.**

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

**12. Unlawful Activities (Prevention) Act, 1967**

**Freezing of Assets under Section 51A -**The Bank will strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex III) and ensure meticulous compliance to the Order issued by the Government.

Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

The details of the two lists are as under:

(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at

https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/1267.pdf

(b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at http://www.un.org/sc/committees/ 1988/list.shtml.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

**13. Jurisdictions that do not or insufficiently apply the FATF Recommendations**

(i) The Bank will 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 will also

consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations.

(ii) The Bank will 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.

Explanation: The process referred to in Section 13(i) & (ii) do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(iii) 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 shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

**14. Branches and subsidiaries outside India**

This policy shall also apply to the branches, subsidiaries and majority owned joint ventures located abroad, to the extent local laws permit. Based on this policy, each foreign office is required to put in place an Anti- Money Laundering Policy (duly approved) which shall also contain the KYC guidelines and Suspicious Activity Reporting (SAR) Procedures as may be required by the rules and regulations of the host country.

**15. Correspondent Banking**

(i) This policy will apply to our dealings with correspondent banks. For correspondent banking relationship an appropriate due diligence procedure will be laid down keeping in view KYC standards existing in the country where the correspondent bank is located and the track record of the correspondent bank in the fight against money laundering and terrorist financing.

(ii) Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

(a) Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.

(b)Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.

(c) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.

(d) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.

(e) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(f) We will ensure that we do not enter into any relationships with 'shell banks' and before establishing any correspondent banking relationship with any foreign institution, branches should take appropriate measures to satisfy themselves that the foreign correspondent institution does not permit its accounts to be used by shell banks. A shell bank is a financial institution which does not have any physical presence in any country.

(g) Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(h) Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

**16. Wire Transfer**

When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

**A) Cross-border wire transfers:**
We will ensure (where both the originator and beneficiary are banks or financial institutions) the following while effecting wire transfer:

i) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number in the absence of an account, as prevalent in the country concerned in the absence of account.

Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.

ii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (i) above

iii) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

iv) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-

cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.

v) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

vi) A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

vii) The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

viii) All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities on receiving such requests.

ix) Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

x) Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.

xi) The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

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

C) Role as Ordering, Intermediary and Beneficiary bank

**Ordering Bank**

As ordering bank for a wire transfer, we shall ensure that qualifying wire transfers contain complete originator information. We must also verify and preserve the information at least for a period of five years.

**Intermediary bank**

i. As Intermediary Bank processing an intermediary element of a chain of wire transfers, for both cross-border and domestic wire transfers, we will ensure that all originator information accompanying a wire transfer is retained with the transfer.

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

**Beneficiary bank**

i. As beneficiary bank for a wire transfer, we will put in place systems to identify wire transfers lacking complete originator information.

ii. 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.

iii. As a beneficiary bank, we should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter.

iv. If the ordering bank fails to furnish information on the remitter, we should consider restricting or even terminating its business relationship with the ordering bank with the approval of the Board.

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

"Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1)(aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.

**The Central KYC Registry is envisaged to be a digital data storehouse having facility of back end verification of documents**. In pursuance of the announcement in the Union Budget 2012-13 to establish a Central KYC Registry (CKYCR), IBA vide Circular No.Cir/RB-CKYC/949 dated 20/06/2015, communicated a direction from Reserve Bank of India, to circulate the common template prepared under the proposed CKYCR amongst the member banks, advising to **prepare their systems and do a pilot run** by furnishing the customer information in the **'common template'** and upload the KYC data together with the photographs of the customer to the Central Registry of CERSAI database.

18. **'Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)**

"FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

FFIs are required to periodically report information on accounts of US persons, who maintain balances above a threshold. In the event of default in the reporting of information on accounts of US taxpayers, a withholding of 30% of the payment made from US sources will be imposed on the recalcitrant account holders and non-participating Financial Institutions.

The monitoring and compliance are done by Income Tax (IT) Department and RBI. Non-compliance of FATCA and CRS will lead to imposing of penalty, by IT dept vide section 271FA and 271FAA of the IT act,1961, and will also affects the bank's Reputation Risk.

19. **Designated Director:**

Prevention of Money Laundering (Maintenance of Records) Rules, 2005 has been recently amended and as per rule 7(1) of it, "every reporting entity shall communicate to the

Director the name, designation and address of the Designated Director and the Principal Officer"

Board has approved Mr.V G Mathew, MD & CEO as the Designated Director for PMLA and stands duly communicated to FIU-IND.

20. **Principal Officer (Money Laundering Reporting Officer)**

(i) Bank will designate a senior officer as Principal Officer who shall be responsible for implementation of and compliance with this policy.

(ii) The Principal Officer will act independently and report directly to the senior management or to the Board of Directors.

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

(iv) 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.

(v) Further, the role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes, all transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to FIU-IND and Cross Border Wire Transfers of value more than 5 lakhs.

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

**21. Maintenance and preservation of records**

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

i. In terms of PML Amendment Act 2012 notified on February 15, 2013, banks 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.

ii. Branches should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving

licenses, PAN card etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.

iii. Banks will pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background including all documents/office records/memorandums pertaining to such transactions and purpose thereof.

iv. Should, as far as possible, be examined and the findings at branch as well as Principal Officer level should also be properly recorded.

iv. Such records and related documents will be made available to auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities, on demand.

v. Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005)

vi. Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it was denominated;
(iii) the date on which the transaction was conducted; and
(iv)the parties to the transaction.

vii. Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities

viii. Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

22.**Employee's Training/Employee's Hiring**

**A) Employees' Training:**

On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy and procedures. All employee training programmes will have a module on KYC Standards and AML Measures. The focus of the KYC/AML Training sessions shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education.

**B) Hiring of Employees**

The Bank will put in place adequate screening mechanism as an integral part of recruitment / hiring process of personnel.

**21.Review of the Policy**

The policy will be reviewed at yearly intervals or as and when considered necessary by the Board.

**********

**ANNEX – I**

**(a)DOCUMENTS TO BE OBTAINED FROM INDIVIDUALS FOR ID PROOF:-**

| PROOF REQUIRED FOR WHAT | NAME OF THE DOCUMENT TO BE OBTAINED |
|---|---|
| 1) Legal Name<br><br>2) Any other names used<br><br>3) Address proof<br><br>Telephone/Mobile phone/email ID | (i) passport<br>(ii) driving license<br>**(iii) Permanent Account Number (PAN) Card**<br>**(iv) Voter's Identity Card issued by Election Commission of India**<br>(v) job card issued by NREGA duly signed by an officer of the State Government<br>(vi) letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number<br>**or any document as notified by the Central Government in consultation with the regulator.** |

**(b)Documents To Be Obtained From Low Risk Customers For Id Proof:-**

| |
|---|
| i) Identity card with applicant's Photograph issued by Central/ State Government Departments, Statutory / Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions: |
| ii) Letter issued by a gazette officer, with a duly attested photograph of the person |

**(c)DOCUMENTS TO BE OBTAINED FROM COMPANIES :-**

| PROOF REQUIRED FOR WHAT | NAME OF THE DOCUMENT TO BE OBTAINED |
|---|---|
| i) Name of the company<br><br>ii) Principal Place of Business<br><br>iii)Mailing Address of the company<br><br>Telephone /mobile phone email ID | i) Certificate of Incorporation<br>ii) Memorandum of Association<br>iii) Articles of Association.<br>iv) Resolution of the Board of Directors to open the account<br>v) Customer identification documents of those who have the authority to operate the account.<br>vi) Power of Attorney granted to its managers, officers or employees to transact business on its behalf.<br>vii) Copy of Pan Card/ Copy of PAN Allotment Letter.<br>viii) Copy of the Telephone Bill<br>ix)List of Directors<br>x)Customer identification documents of directors<br>xi) List of Beneficiary owners<br>xii) Customer identification documents of BOs |

**(d) DOCUMENTS TO BE OBTAINED FROM PARTNERSHIP FIRMS :-**

| PROOF REQUIRED FOR WHAT | NAME OF THE DOCUMENT TO BE OBTAINED |
|---|---|
| i) Legal Name<br>ii) Address<br>iii) Names of all partners and their addresses<br>iv) Telephone Numbers of the firm and partners | i) Registration Certificate, if registered.<br>ii) Partnership Deed.<br>iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf.<br>iv) Proof of ID and Proof of Address of the Partners and POA holders<br>v) Telephone Bill in the name of the firm<br>vi) List of Beneficiary owners<br>vii) Customer identification documents of BOs |

**(e) DOCUMENTS TO BE OBTAINED FOR ACCOUNTS OF TRUSTS & FOUNDATIONS**

| PROOF REQUIRED FOR WHAT | NAME OF THE DOCUMENT TO BE OBTAINED |
|---|---|
| i) Names of trustees, settlors, beneficiaries and signatories<br>ii)Names and addresses of the founder, the managers/directors and the beneficiaries<br>iii) Telephone/Fax Numbers | i) Certification of Registration, if registered.<br>ii) Power of Attorney granted to transact business on its behalf.<br>iii)Any officially valid document to identify the trustees, settlors , beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses.<br>iv) Resolution of the managing body of the foundation/ association.<br>v) Telephone Bill. |

**(f) DOCUMENTS TO BE OBTAINED FOR ACCOUNTS OF SOLE PROPREITORSHIP CONCERNS :**

| PROOF REQUIRED FOR WHAT | NAME OF THE DOCUMENT TO BE OBTAINED |
|---|---|
| Proof of name, address and activity of the concern | i) Registration Certificate (in the case of a registered concern.).<br>ii) Certificate/License issued by the Municipal Authorities under the Shop & Establishment Act. iii) Sales and Income Tax Returns. iv) CST/VAT Certificate.<br>v) Certificate/registration document issued by Sales Tax /Service Tax / Professional Tax Authorities.<br>vi) License issued by the Registering Authority like Certificate of Practice issued by the Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/ licensing document issued in the name of the Proprietory concern by the Central Government or State Government Authority/Department etc. Banks may also accept IEC (Importer Exported Code) issued to the proprietory concern by the office of |

| | |
|---|---|
| | DGFT as an identity document for opening of the bank account etc.<br>vii) 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.<br>Viii) Utility Bills such as electricity, water and landline telephone bills in the name of the Proprietory concern.<br>**Any two of the above documents would suffice. These documents should be in the name** |

**E- KYC**

RBI vide Circular No. DBOD.AML.BC. No. 44/14.01.001/2013-14 dated 02.09.2013, approved e-KYC service as a valid process for KYC verification under the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. Thus, the information containing the demographic details and the photographs made available from UIDAI as a result of the e-KYC process (which is in an electronic form and accessible so as to be usable for a subsequent reference) may be treated as an 'Officially valid document' under the PMLA Rules.

Accordingly, branches may accept e-Aadhaar downloaded from the UIDAI website as an officially valid document subject to the following:

(a) If the prospective customer knows only his/her Aadhaar Number, the bank may print the prospective customer's e-Aadhaar Letter in the bank directly from the UIDAI portal; or adopt the e-KYC procedure as mentioned in the circular reference no. DBOD.AML.BC.No.44/14.01.001/2013-14 dated 02.09.2013.
(b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt the e-KYC procedure as mentioned in the circular reference no. DBOD.AML.BC.No. 44/14.01.001/2013-14 dated 02.09.2013 or confirm the identity and address if the resident through simple authentication service of UIDAI.
(c) Physical Aadhaar Card/Letter issued by UIDAI containing details of name, address and Aadhaar Number received through post and the e-KYC procedure as mentioned in the circular reference no. DBOD.AML.BC.No. 44/14.01.001/2013-14 dated 02.09.2013 would continue to be accepted as an 'Officially Valid Document'.