

**Policy Guidelines on KYC/AML/CFT-2019-20 (Domestic Branches).**

**1. OBJECTIVE**

**1.1. Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT)**

The objective of KYC/AML/CFT guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Bank to know/ understand the customers and their financial dealings better and manage the risks prudently. The Board approved policy on KYC/AML/CFT is subject to annual review.

**2. DEFINITIONS**

**2.1 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 includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

**2.2 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 the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company.

**2.3 Officially Valid Documents:**

Officially Valid Document (OVD) means:

1. Aadhaar Card
2. Passport
3. Driving License
4. Voter Identity Card issued by Election Commission of India
5. Job Card issued by NREGA duly signed by an officer of the State Government
6. Letter issued by the National Population Register containing details of name and address
7. Any other document as notified by the Central Government in consultation with the Regulator.

**2.3.1** In respect of low risk category of customers, where simplified measures are applied for verifying the identity of the clients, the following documents shall be deemed to be OVD:

- a) 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;

- b) letter issued by a Gazetted Officer, with a duly attested photograph of the person.

**2.3.2** Further, where simplified measures are applied, for the limited purpose of proof of address, the following additional documents are deemed to be OVDs:

- (a) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);
- (b) Property or Municipal Tax receipt;
- (c) 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, lease 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.

#### **2.4 Person:**

In terms of PML Act a person 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).

#### **2.5 Transaction:**

“Transaction” means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

- (i) opening of an account;
- (ii) 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;
- (iii) the use of a safety deposit box or any other form of safe deposit;
- (iv) entering into any fiduciary relationship;
- (v) any payment made or received in whole or in part of any contractual or other legal obligation; or
- (vi) establishing or creating a legal person or legal arrangement.

### **3. KEY ELEMENTS OF KYC POLICY:**

The KYC Policy includes the following four key elements:

- a) Customer Acceptance Policy (CAP);
- b) Customer Identification Procedures (CIP);

- c) Monitoring of Transactions; and
- d) Risk Management.

### **3.1 Customer Acceptance Policy (CAP)**

Bank shall develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the Bank and including the following aspects of customer relationship in the Bank.

- (i) No account is opened or maintained in anonymous or fictitious / benami name.
- (ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Bank in categorizing the customers into low, medium and high risk ones, as detailed in para 3.1.1;
- (iii) Documents and other information to be collected from different categories of customers are detailed in Annexure-III of this Note.
- (iv) Bank will not open an 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 required documents either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. Bank may also consider closing an existing account under similar circumstances.
- (v) Circumstances in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking.
- (vi) Bank shall have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

Adoption of customer acceptance policy and its implementation shall not become too restrictive, which result in denial of banking facility to the members of the general public, especially to those, who are financially or socially disadvantaged.

#### **3.1.1 Risk Perception in respect of Customer:**

"Customer Risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by the customer.

For categorizing a customer as Low Risk, Medium Risk and High Risk, the parameters considered are customer's identity, social/financial status, nature of business activity, information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

#### **Low Risk Customers (Level 1 customers):**

Individuals (other than High Networth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as Low Risk, such as:

- Salaried employees
- People belonging to lower economic strata of the society
- Government Departments

- Government owned companies
- Regulatory and Statutory bodies, etc.

For the above category, the KYC requirements of proper identification and verification of proof of address would suffice.

**Medium Risk Customers (Level 2 customers):**

Customers who are likely to pose a higher than average risk to the Bank should be categorised as medium or high risk.

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her client profile, etc. besides proper identification.

The following customers are classified as **Medium Risk Customers:**

- Gas Dealers
- Car/boat/plane dealers
- Electronics (wholesale)
- Travel agency
- Telemarketers
- Telecommunication service providers
- Pawnshops
- Auctioneers
- Restaurants, Retail shops, Movie theatres, etc.
- Sole practitioners
- Notaries
- Accountants
- Blind
- Purdanashin

**High Risk Customers (Level 3 customers):**

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank shall subject such accounts to **enhanced monitoring on an ongoing basis.**

- Trusts, charities, NGOs and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'.
- Accounts under Foreign Contribution Regulation Act.
- Politically Exposed Persons (PEPs).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers.
- High Net worth Individuals\*
- Non-Resident customers.
- Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewelers.

**\* Parameters for defining High Net worth Individuals:**

Customers with any of the following:

- 1) Average balance of Rs. 100 lakh and above in all deposit accounts (SB+CA+TD).
- 2) Enjoying Fund based limits/term loans exceeding Rs. 100 lakh.

The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Branch/Office.

Branches shall prepare a Risk profile of each customer and apply enhanced due diligence measures on High Risk customers. IBA has provided an indicative list of High/Medium Risk Products, Services, Geographies, Locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure IV of this Note).

### **Customer Risk Categorisation**

As per IBA Working Group guidelines, Bank may choose to carry out either manual classification or automatic classification or a combination of both. Similarly for selecting parameters, Bank may select the parameters based on the available data. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter.

Bank has adopted combination of manual and automatic classification. Based on the availability of data, Bank shall finalise parameters which are available in the system and the same shall be reviewed annually. System shall assign provisional risk categorization based on the system provided parameters. Branches shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy.

Branches shall prepare a profile for all Customers based on risk categorization. The Customer profile may contain information relating to Customer's identity, social/financial status, nature of business activity, information about his client's business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. Risk categorization shall be done based on selected parameters and assigning suitable risk category.

### **Risk Parameters**

The first step in process of risk categorization is selection of parameters, which would determine customer risk.

IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used, to determine the profile and risk category of Customers:

1. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
2. Business Segment : Retail, Corporate etc.
3. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national.
4. Product Subscription: Salary account, NRI products etc.
5. Economic Profile: HNI, Public Ltd. Company etc.
6. Account Status: Active, inoperative, dormant.
7. Account Vintage: Less than six months old etc.
8. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.
9. Suspicious Transaction Report (STR) filed for the customer.
10. AML alerts.

Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc. can also be used in addition of the above parameters. Bank shall adopt all or majority of these parameters based on availability of data.

**Risk rating of Customers:**

Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of origin, sources of funds and client profile etc.

A. An Illustrative list of Low/Medium/High Risk Customers, Products, Services, Geographies, etc., based on the recommendations of IBA Working Group on Risk Based Transaction Monitoring is detailed in Annexure IV of this Note.

B. Risk rating based on the Deposits/account balance:

<i>Account Types</i>	<i>High</i>	<i>Medium</i>	<i>Low</i>
All deposit accounts (SB+ CA+ TD)	Rs.100 lakh & above	Rs. 25 lakh & above but less than Rs.100 lakh	Less than Rs.25 lakh

Above categorization of the Customer shall be based on all accounts linked to Customer ID irrespective of constitution of account like Joint account, Partnership account etc. However accounts linked to Customer ID where customers do not have any stake in Business/activity need not be clubbed for the above purpose.

C. Risk Categorisation of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

- Unusual transaction/behavior (given as Annexure V - Monitoring of Customer Risk Categorisation (CRC)).
- Submitted Suspicious Transaction Reports (STR) for Customer.
- Submitted Cash Transaction Report (CTR).
- Frequent Cheque returns.

D. Risk Categorisation of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer. Example: a Travel Agent (Medium risk) with Proprietorship account (low risk) and having Savings account with average balance of Rs.1,50,000/- (medium risk) and Term Deposit of Rs.4,00,000/- (low risk) , shall be assigned with overall rating of "Medium Risk", provided all other conditions mentioned under C above does not necessitate for assigning "High Risk".

**Risk categorization of Customers undertaken by the Bank:**

Based on the policy/guidance notes of RBI/IBA and also the methodology of Customer Risk Categorisation provided by ORM Department (as detailed under points A, B, C & D above), risk rating has been assigned taking into account the following parameters available in CBS system :

- Customer type.

- Customer profession.
- Type of business.
- Product code.
- Account status
- Account vintage.
- Average balance in deposits in SB/Current/Term Deposit accounts.

All customer profiles/accounts of NRIs, HNIs, PEPs, NGOs, Trusts, Co-operative Societies, HUF, Exporters, Importers and Accounts having Beneficial Owners shall be invariably categorised as High Risk, irrespective of the lower risk category (low/medium) allotted under other parameters in the Matrix like customer profession, type of business, product code, account status, account vintage and balance in the account.

As per RBI directions, the parameters used for categorising the risk profile of customers should include those named in complaints (from legal enforcement authorities)/frauds. As the system will not identify the customers/accounts named in complaints (from legal enforcement authorities)/frauds, this parameter has not been included in the Risk Categorisation Matrix. Branches are advised to categorise such customers/ accounts under “High Risk” category as and when complaints (from legal enforcement authorities) are received or fraud is reported against the customer/account holder.

Blocked Accounts and Unclaimed deposits shall be categorised as High Risk. As per RBI directions, Blocked account status should be part of the initial categorisation of an account at the branch level rather than being part of the review of risk categorisation at the central level. Hence, branches are advised to categorise such accounts as High Risk at the time of blocking the account.

Accounts of dealers in jewellery, gold/silver/bullions, diamonds and other precious metals/stones shall be categorised under High Risk.

Under vintage parameter, newly opened CASA accounts which have not completed 6 months shall be categorised as High Risk, except accounts pertaining to staff, ex-staff, pensioners, small accounts, Financial Inclusion and Basic Savings Bank Accounts. However, if the accounts under the above categories are rated as High/Medium risk under any of the other 6 parameters under the risk categorization matrix, such accounts are to be categorized basing on the highest risk category allotted under those parameters.

**THE ROLES AND RESPONSIBILITIES OF AUTHORITIES FOR CUSTOMER RISK CATEGORISATION (CRC):**

**Roles and responsibilities of Branches:**

Branches shall review Customer risk categorization based on the risk categorization generated by the system, every six months, as on 15th of May and November every year.

Branches may also apply additional alert indicators to address specific risks faced by them.

**Roles and responsibilities of Circle Offices:**

Shall monitor/follow-up process of review/classification/re-classification of Customer Risk Categorisation.

Shall ensure compliance of Risk Categorization at branches every six months by obtaining confirmation from ROs and branches under direct control of CO.  
Shall submit periodical reports on implementation/review of risk categorisation to RBS & MIS Wing, H.O.  
Shall attend/follow-up audit observations/remarks.

**Roles and responsibilities of Regional Offices:**

Shall monitor/follow-up process of review/classification/re-classification of Customer Risk Categorisation.  
Shall ensure compliance of Risk Categorization at branches every six months.  
Shall submit periodical reports on implementation/review of risk categorisation to Circle Office.  
Shall attend/follow-up audit observations/remarks.

**Development Section, SP&D Wing, H.O:**

Oversee implementation/monitoring and review of risk categorization of customers by putting in place suitable reporting/monitoring mechanism.  
Ensure proper maintenance of MIS for customer risk categorization and migration data.  
Shall review fixing of parameters available through the system annually.  
SP&D Wing along with DIT Wing, shall identify the parameters available in the system for risk categorization through the system as per the model suggested in the policy.

**RBS & MIS Wing, H.O:**

Shall review and provide necessary recommendations/directions to strengthen adherence of KYC/AML guidelines.  
Shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

**Monitoring/Review of Customer Risk Categorisation (CRC):**

Branches shall carry out a review of risk categorization of customers at a periodicity of not less than once in six months i.e., as on 15th of May and November every year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.

Wherever there is suspicion at branch level that a Customer is above low risk, branches should carry out customer due diligence (CDD).

While monitoring of transactions, branches shall arrive at a conclusion whether the transaction is suspicious or not, based on objective parameters for enhanced due diligence. Some of the objective parameters for enhanced due diligence could be:

- Customer locations.
- Financial Status.
- Nature of business.
- Purpose of transaction.

## **3.2 Customer Identification Procedure (CIP)**

### **3.2.1 General**

(a) Customer identification means undertaking Client Due Diligence (CDD) measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs.

Bank shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of banking relationship. The Bank shall observe due diligence based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).

- (b) Bank shall have a policy approved by the Board which clearly spells out the Customer Identification Procedure to be carried out at different stages, i.e.,
- i. While establishing a banking relationship;
  - ii. While carrying out a financial transaction;
  - iii. When the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;
  - iv. When bank sells third party products as agent;
  - v. While selling Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000/-.
  - vi. When carrying out transactions for a non-account based customer, that is a walk-in-customer, where the amount is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected;
  - vii. When the Bank 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/-.

'Mandatory' information required for KYC purpose which the customer is obliged to give while opening an account should be obtained at the time of opening the account/ 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.

### **3.2.2 (I) Customer Due Diligence requirements (CDD) while opening accounts**

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

Branches shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

The 'live run' of the CKYCR would start in phased manner. Accordingly, in the first phase, branches shall upload the KYC data with CERSAI, in respect of new individual accounts opened during the day. Bank shall prepare a plan for uploading the data in respect of existing individual accounts into CKYCR server.

#### **A. Accounts of individuals:**

Where the client is an individual, he shall submit:-

- (i) Any Officially Valid Document which contains proof of identity/address.**
- (ii) The Permanent Account Number (PAN) or Form 60 as defined in the Income Tax Rules, 1962,

And such other documents including in respect of the nature of business and financial status of the client as may be required by the Bank.

- Officially Valid Documents (OVD) are as under:

- 1) Aadhaar Card
- 2) Passport
- 3) Driving License
- 4) Voter Identity Card issued by Election Commission of India
- 5) Job Card issued by NREGA duly signed by an officer of the State Government
- 6) Letter issued by the National Population Register containing details of name and address
- 7) Any other document as notified by the Central Government in consultation with the Regulator.

#### **(ii) e-KYC services of UIDAI**

In order to reduce the risk of identity fraud, document forgery and to have paperless KYC verification, UIDAI has launched its e-KYC service. The Reserve Bank of India has directed the banks to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process (which is in an electronic form and accessible so as to be usable for a subsequent reference) shall be treated as an “Officially Valid Document” under PML Rules.

- ***Branches can continue to seek e-KYC based authentication of those beneficiaries who are availing subsidies/benefits/services covered by section 7 of the Aadhaar Act.***
- ***e-KYC authentication facility can also be continued to be permitted for those customers who give a declaration that s/he is desirous of receiving her/his entitled benefits or subsidies of welfare schemes covered by section 7 of the Aadhaar Act.***
- ***For other customers, Branches can use physical copy of the Aadhaar card as well as e-Aadhaar, masked Aadhaar and offline electronic Aadhaar xml provided by UIDAI, which are various forms of Aadhaar, as Officially Valid Documents (OVD) for the KYC purpose.***

***(As per UIDAI circular dated 23-10-2018 based on the opinion received from the Ld. Attorney General for India after the Aadhaar Judgment of the Hon. Supreme Court of India, delivered on 26-09-2018).***

**(iii) Introduction of accounts:**

Since introduction from an existing customer is not necessary for opening accounts under PML Act and Rules or the RBI's extant instructions, branches shall not insist on introduction for opening of bank accounts. After passing of PML Act and introduction of document based verification of identity/address of the proposed account holders, the accounts opened with proper documents are considered as acting in good faith and without negligence by the banks.

**(iv) Simplified Measures for Proof of Identity:**

If an individual customer does not have Aadhaar or PAN or any of the OVDs (as mentioned in para 2.3 as proof of identity, then 'simplified measures' shall be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any one of the documents referred under para 2.3.1, which will be deemed as an OVD for the purpose of proof of identity.

**(v) Simplified Measures for Proof of Address:**

The additional documents mentioned under para 2.3.2 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.

**(vi) Accounts of married woman:**

As per the amendment to the Rules, 2005 (Gazette notification dated 22.09.2015), a document shall be deemed to an "officially valid document" even if there is a change in the name subsequent to its issuance, provided it is supported by a marriage certificate issued by the State Government or a Gazette notification, indicating such a change of name.

Accordingly, Branches shall accept a copy of 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 while establishing an account based relationship or while undergoing periodic updation exercise.

**(vii) Small Accounts:**

It has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce OVDs to satisfy the Bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. In such cases, if a person who wants to open an account and is not able to produce any of the OVDs or the documents applicable in respect of simplified procedure, bank shall open a "small account". The small accounts can be opened under "Canara Small Savings Bank Deposit Account".

The "Canara Small Savings Bank Deposit" account can be opened by production of a self attested photograph and affixation of signature or thumb impression, as the case may be, on the Account Opening form. The designated bank official, while opening

the small account, should certify under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence.

The features of the above account and restrictions stipulated by RBI/Govt. of India are as follows:

- accounts where aggregate of all credits in a financial year does not exceed Rs.1.00 lac;

- the aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000/- and

- where the balance at any point of time does not exceed Rs.50,000/-.

Any violation of the stipulations mentioned above will result in restraining the operations in the account after giving due notice to the account holder.

A Canara Small Savings Bank Deposit Account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the Bank of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.

The 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 +

Foreign remittances shall not be allowed to be credited into a Canara Small Savings Bank Deposit Account unless the identity of the customer is fully established through the production of officially valid documents.

#### **(viii) Basic Savings Bank Deposit Accounts**

The “Basic Savings Bank Deposit Account” shall offer following minimum common facilities to all the customers:

- a) The Basic Savings Bank Deposit Account shall be considered a normal banking service available to all.
- b) This account shall not have the requirement of any minimum balance.
- c) The services available in the account will include deposit and withdrawal of cash at bank branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.
- d) While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a maximum of four withdrawals in a month, including ATM withdrawals; and
- e) Facility of ATM card or ATM-cum-Debit Card.

The above facilities will be provided without any charges. Further, no charge will be levied for non-operation/ activation of inoperative Basic Savings Bank Deposit Account. Additional value added services beyond the stipulated basic minimum services will be chargeable.

The Basic Savings Bank deposit Account would be subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time. If such account is opened on the basis of simplified KYC

norms, the account would additionally be treated as a “Small Account” and would be subject to conditions stipulated for such accounts as detailed under para 3.2.2 A (vii).

Holders of Basic Savings Bank Deposit Account will not be eligible for opening any other savings bank deposit account in the Bank. If a customer has any other existing savings bank deposit account in the Bank, he/she will be required to close it.

(ix) A customer is required to submit only one Officially Valid Document (OVD) for both proof of identity and for proof of address 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.

(x) 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 shall 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 shall be verified by the branch through ‘positive confirmation’ such as acknowledgment 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 for correspondence to the Bank within two weeks of such a change.

(xi) In case the address mentioned as per ‘proof of address’ undergoes a change, fresh proof of address should be submitted to the branch within a period of six months.

(xii) 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, Branches shall obtain an 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 him/her.

(xiii) Branches are 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. KYC once done by one branch of the Bank shall 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. The customer shall be allowed to transfer his account from one branch to another branch without restrictions.

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.

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 proof of address for the purpose.

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

(xv) For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the branch may rely on a third party; subject to the conditions that-

(a) the branch immediately obtains necessary information of such client due diligence carried out by the third party;

(b) the branch 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;

(c) the branch 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;

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

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

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

With the introduction of 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 (i.e., customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank), apart from applying the usual customer identification procedures, there shall be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents may be called for. In such cases, Bank may also require the first payment to be effected through the customer's account with another bank which, in turn, follows KYC procedures. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the Bank may have to rely on third party certification. In such cases, it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

**(xvii) Accounts of Foreign students studying in India:**

Considering that foreign students arriving in India are facing difficulties in complying with the Know Your Customer (KYC) norms while opening a bank account due to non-availability of any proof of local address, the following procedure shall be followed for opening accounts of foreign students who are not able to provide an immediate address proof while approaching the Bank for opening bank account:-

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

b) Branches should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.

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

- d) The account would be treated as a normal NRO account after verification of address and will be operated in terms of existing guidelines issued in the Manual of instructions on Non-Resident Deposits and Circulars issued from time to time.
- e) Students with Pakistani nationality will need prior approval of the Reserve Bank of India for opening the account.

**(xviii) 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/ Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Bank shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. Branches shall maintain a database of PEP accounts in the Branch. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming a Politically Exposed Person (PEP), has to be taken by branch head in branches headed by Scale IV and above. For all other branches, the decision is to be taken by the executive overseeing MIPD & PP Section of the respective Regional Office/Circle Office.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where a PEP is the ultimate beneficial owner shall be categorized as 'High Risk' so that appropriate transaction alerts are generated and the accounts are subjected to enhanced CDD on an ongoing basis.

Bank shall have appropriate ongoing risk management systems 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.

**B. Accounts of persons other than individuals:**

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

**(i) Accounts of Companies**

Where the client is a company, certified copies of following documents are to be submitted:

- (i) Certificate of incorporation
- (ii) Memorandum and Articles of Association
- (iii) A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf.

- (iv) (a) ***Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. and***
  - (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to managers, officers or employees holding an attorney to transact on the company's behalf.

**(ii) Accounts of Partnership firms**

Where the client is a partnership firm, certified copies of following documents are to be submitted:

- (i) Registration Certificate
- (ii) Partnership Deed
- (iii) (a) ***Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. and***
  - (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the partnership firm.

**(iii) Accounts of Trusts**

Where the client is a Trust, certified copies of following documents are to be submitted:

- (i) Registration Certificate
- (ii) Trust Deed
- (iii) (a) ***Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. and***
  - (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the Trust.

**(iv) Accounts of Unincorporated association or a body of individuals:**

Where the client is an unincorporated association or a body of individuals, certified copies of following documents are to be submitted:

- (i) Resolution of the managing body of such association or body of individuals
- (ii) Power of Attorney granted to the person who will transact on its behalf.
- (iii) (a) ***Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. and***
  - (b) PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the unincorporated association or a body of individuals.

**(v) Accounts of Proprietary Concerns**

For Proprietary concerns, in addition to the Officially Valid Documents applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern should be submitted:

- a) Registration Certificate (in the case of a registered concern).
- b) Certificate / licence issued by the Municipal authorities under Shop & Establishment Act.
- c) Sales and income tax returns.
- d) CST / VAT certificate.

- e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
- f) Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- g) 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.
- h) Utility bills such as electricity, water and landline telephone bills.
- i) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

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 branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, 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.

**(vi) For opening accounts of Government or its Departments, Societies, Universities and Local Bodies like Village Panchayats, a certified copy of the following documents shall be obtained:**

- i. Document showing name of the person authorized to act on behalf of the entity;
- ii. (a) ***Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf.*** and
  - (b) PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the entity.
- iii. Such documents as may be required by the Bank to establish the legal existence of such an entity/ juridical person.

**(vii) Accounts of Foreign Portfolio Investors (FPIs) for Portfolio Investment Scheme (PIS):**

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 bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank would be required. Category-I FPIs are not required to submit the undertaking that upon demand by the Regulators/ Law Enforcement Agencies the relative document/s would be submitted to the bank.

For this purpose, branches 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.

SEBI will advise Custodians/Intermediaries regulated by them to share the relevant KYC documents with the banks concerned based on written authorization from the FPIs. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to the Custodians/Regulated Intermediaries may be transferred to the concerned

bank through their authorised representative. While transferring such documents, the Custodian/Regulated Intermediary shall certify that the documents have been duly verified with the original or notarised documents have been obtained, wherever applicable. In this regard, proper records of transfer of documents have to be maintained, both at the level of the Custodian/Regulated Intermediary as well as at the bank, under signatures of the officials of the transferor and transferee entities.

While opening bank accounts for FPIs in terms of the above procedure, branches are ultimately responsible for the customer due diligence done by the third party (i.e. the Custodian/Regulated Intermediary) and need to take enhanced due diligence measures, as applicable, if required. Further, branches are required to obtain undertaking from FPIs or a Global Custodian acting on behalf of the FPI to the effect that as and when required, the exempted documents will be submitted.

In order to facilitate secondary market transactions, the branches may share the KYC documents received from the FPI or certified copies received from a Custodian/Regulated Intermediary with other banks/regulated market intermediaries based on written authorization from the FPI.

The above guidelines are applicable for both new and existing FPI clients. These guidelines are applicable only for Portfolio Investment Scheme (PIS) by FPIs. In case the FPIs intend to use the bank account opened under the above procedure for any other approved activities (i.e. other than PIS), they would have to undergo full KYC exercise.

#### **(viii) Client accounts opened by professional intermediaries**

When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client shall be identified. Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank. 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 shall be identified. Where such funds are co-mingled at the Bank, the Bank shall still look into the beneficial owners. Where the Bank rely on the 'customer due diligence' (CDD) done by an intermediary, Bank shall satisfy itself that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. The ultimate responsibility for knowing the customer lies with the Bank.

### **C. Beneficial Ownership**

Rule 9(3) 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 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.

A juridical person is an Entity, that is not a single natural person(as a human being), authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).

The procedure for determination of Beneficial Ownership as per RBI/Government guidelines 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/have a controlling ownership interest or who exercises control through other means.

Explanation.- For the purpose of this sub-clause-

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

2. "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;

(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, 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; and

(f) 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.

There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, Bank shall determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, Bank shall 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 shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

#### **D. Accounts of Non Profit Organisations**

A Non Profit Organisation (NPO) means 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 8 of the Companies Act 2013. All transactions involving receipts by these NPOs of value more than Rs.10 lac or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 lac, the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

**E. Accounts operated by Power of Attorney Holders/Letter of Authority Holders:**  
In case of accounts operated by Power of Attorney (POA) Holders / Letter of Authority (LOA) Holders, KYC documents shall be obtained from such POA holders/ LOA holders and records shall be maintained/ updated in the system.

**II. Introduction of New Technologies - Credit cards / debit cards / smart cards / gift cards etc.**

Bank shall pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. The Electronic Cards (debit card, credit card, etc.) issued by the Bank to the customers may be used by them for buying goods and services, drawing cash from ATMs and electronic transfer of funds.

Bank shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Bank shall ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, where marketing of these cards is done through the services of agent, the agents will also to be subjected to due diligence KYC measures.

**III Periodic updation of KYC**

**A. CDD requirements for periodic updation:**

Bank shall have a system of periodical updation of customer identification data (including photograph/s) as under:

(i) Branches should apply client due diligence measures/full KYC exercise to existing clients at least every two years for High Risk customers, every eight years for Medium Risk customers and every ten years for Low Risk customers taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

Full KYC exercise may include all measures for confirming identity and address and other particulars of the customer that the Bank may consider reasonable and necessary based on the risk profile of the customer. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

Branches should carry out **ongoing due diligence** of existing clients in order to ensure that their transactions are consistent with the Bank's knowledge of the client, his business and risk profile and where necessary, the source of funds.

Branches should undertake client due diligence (CDD) measures while commencing an account-based relationship. Such measures include identifying and verifying the customer and beneficial owner on the basis of reliable and independent information and data or documents.

The periodical verification/updation of customer data shall be done irrespective of whether the account has been transferred from one branch to another and Bank shall maintain records of transactions as prescribed.

Apart from home branches, the branches other than Home (Base) Branch also shall perform Full KYC exercise/ Positive confirmation, whenever the customer approaches that branch and requests the branch to complete the Full KYC exercise/Positive confirmation by submitting the required documents. Such branches should exercise

due diligence in verification of the documents and updation of the details in the CBS system.

(ii) Branches need not seek fresh proofs of identity and address at the time of periodic updation from those customers who are categorised as 'low risk', in case of 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. Branches need not insist on physical presence of such low risk customer at the time of periodic updation.

(iii) Fresh photographs and Officially Valid Documents shall be obtained from minor customer on becoming major.

## **B. Freezing and Closure of accounts**

It would always be open to the Bank to close the account of KYC non-compliant customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken by the Branch-in-charge.

While it is absolutely necessary for banks as well as customers to comply with the measures prescribed for KYC/AML purposes, drastic measures like closing of accounts may be taken only after sending out sufficient discernible warning signals to the customers, basing on the level of customer education and public awareness on the subject. In all such cases where the account holders are either not responding over a period of time/not found at the given address, Bank may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

Before taking the extreme step of closing an account on account of noncompliance with the KYC/AML requirements, as an initial measure, branches are advised to place such accounts under close watch, depriving the non-compliant customers certain additional facilities, till the customer complies with such requirements.

This exercise, however, should not extend beyond a period of three months. If the customer despite such measures, shows unwillingness to comply with KYC/AML/ CFT requirements, branches would be free to proceed further and close the accounts after giving due notice to him/her. It is reiterated that basic banking transactions already in force should not be disturbed for meeting KYC review requirements.

In case of non-compliance of KYC requirements by the customers despite repeated reminders by branches, branches should impose "partial freezing" on such KYC non-compliant accounts in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing "partial freezing", branches are advised 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 and followed by a reminder for further period of three months. Thereafter, branches to 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", branches should disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the branches to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken by the Branch-in-charge.

In the Circumstances when the Bank believes that it would no longer be satisfied about the true identity of the account holder, the Bank shall file a Suspicious Transaction Report (STR) with Financial Intelligence Unit India (FIU-IND) under the Department of Revenue, Ministry of Finance, Government of India.

#### **IV Miscellaneous**

##### **A. At par cheque facility availed by co-operative banks**

Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in-customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, branches maintaining/opening such accounts should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, branches should retain the right to verify the records maintained by the client cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements.

##### **B. Operation of Bank Accounts & Money Mules**

Money Mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering. "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 order to minimize the operations of such mule accounts, Branches should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

##### **C. Simplified norms for Self Help Groups (SHGs):**

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening Savings Bank accounts and credit linking of their accounts, following simplified norms shall be followed by branches:

- (a) KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.
- (b) As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary.

##### **D. Walk-in Customers**

In 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 shall be verified.

If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/-, the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND. The identity and address of the Walk-in customer shall be verified by obtaining KYC documents and records are to be maintained/ updated in the system. Bank shall also verify the identity of the customers for all international money transfer operations.

#### **E. Issue of Demand Drafts, etc., for more than Rs. 50,000/-**

Any remittance of funds by way of Demand Draft or any other mode and issue of Traveller's cheques for value of Rs. 50,000/- and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Bank shall not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

***The name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheques etc by the issuing Bank with effect from 15<sup>th</sup> September 2018.***

#### **F. Unique Customer Identification Code**

A Unique Customer Identification Code (UCIC) will help the Bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Bank to have a better approach to risk profiling of customers. Branches are required to strictly avoid creating multiple customer IDs while opening new accounts and in case of existing multiple IDs, branches have to carry out the process of de-duplication.

#### **G. Prohibition on dealing in Virtual Currencies (VCs).**

- 1. Entities regulated by the RBI shall not deal in VCs or provide services for facilitating any person or entity in dealing with or settling VCs with immediate effect.***
- 2. Regulated entities which already provide such services shall exit the relationship within three month from the date of RBI circular.***

### **3.3 Monitoring of Transactions:**

Ongoing monitoring is an essential element of effective KYC/AML procedures. Branches should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

(a) The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

(b) Branches should pay particular attention to the following types of transactions:

(i) Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

(ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.

(iii) Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

(iv) High account turnover inconsistent with the size of the balance maintained.

(c) Bank shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months.

(d) Branches should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Branches should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the branches and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

e) Supervisors should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt, necessary enquiries should be made with the account holders.

f) While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.

g) Branches are advised to mandatorily obtain either PAN or Form 60 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs. 50,000/- and above. If the customer appears to be structuring the transactions into a series of transactions below the threshold of Rs. 50,000/-, branches are required to obtain PAN or Form 60 (if PAN is not available) from the customer. Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of obtention of PAN or Form 60, wherever the aggregate amount of transactions is Rs. 50,000/- and above.

h) All the staff members are instructed to maintain the standards of good conduct and behaviour expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

### **3.4 Risk Management**

The inadequacy or absence of KYC standards can subject the Bank to serious customer and counter party risks especially reputational, operational, legal and concentration risks. Reputational Risk is defined as “the potential that adverse publicity regarding the Bank’s business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution”. Operational Risk can be defined as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events”. Legal Risk is “the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank”. Concentration Risk although mostly applicable on the assets side of the balance sheet, may affect the liabilities side as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the Bank’s liquidity. It is worth noting that all these risks are interrelated. Any one of them can result in significant financial cost to the Bank as well as the need to divert considerable management time and energy to resolve problems that arise.

Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, operational and legal risk arising from such accounts, Bank shall aggregate and monitor significant balances and

activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

Branches should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds. The Board of Directors of the Bank shall ensure that an effective KYC/AML/CFT programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters.

In addition, the following also to be ensured for effectively implementing the AML/CFT requirements:

- (i) Using a risk-based approach to address management and mitigation of various AML/CFT risks.
- (ii) Allocation of responsibility for effective implementation of policies and procedures.
- (iii) Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
- (iv) Concurrent/internal audit/snap audit to verify the compliance with KYC/AML policies and procedures.
- (v) Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals and to Board of Directors at monthly intervals by KYC Cell, RBS & MIS Wing.

Branches shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank.

Branches shall categorise the customers into low, medium and high risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The Bank shall have a Board approved policy for risk categorisation and ensure that the same is meticulously complied with, to effectively help in combating money laundering activities. The nature and extent of due diligence, shall be based on the following principles:

- (i) 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, shall be categorised as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc.
- (ii) Customers who are likely to pose a higher than average risk shall be categorised as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, shall be categorised as high risk.

Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the 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 business relationship.

Bank has adopted a risk categorization model as advised by the Indian Banks Association.

**The roles and responsibilities of various Wings and Sections with regard to KYC/AML/CFT matters are as follows::**

**Development Section, SP&D Wing-**

Issuance of guidelines pertaining to KYC/AML/CFT for Domestic deposits and implementation/monitoring of the same in liaison with DIT Wing.

**Overseas Banking Division, International Operations Wing-**

Issuance of guidelines pertaining to KYC/AML/CFT for Overseas deposits and implementation/monitoring of the same in liaison with DIT Wing.

**KYC Cell, RBS & MIS Wing-**

Verification of implementation of KYC/AML/CFT guidelines including liaison with RBI/IBA/FIU/other agencies, reporting to regulatory authorities and AFI team of RBI apart from attending to STR, CTR and CCR alerts.

The Bank shall take steps to identify and assess the Money Laundering /Terrorism Financing risk for customers, as also for products/ services/ transactions/ delivery channels. Bank shall have controls and procedures in place to effectively manage and mitigate the risk adopting a risk-based approach. As a corollary, Bank shall adopt enhanced measures for products, services and customers with a medium or high risk rating.

**4. CORRESPONDENT BANKING AND SHELL BANK**

Correspondent Banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash / funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Bank shall take the following precautions while entering into a correspondent banking relationship:

(a) Bank shall gather sufficient information to fully understand the nature of the 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.

(b) Such relationships may be established only with the approval of the Board or by a committee headed by the MD & CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.

(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, Bank shall satisfy 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.

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

(f) Bank shall be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of Financial Action Task Force (FATF) Recommendations.

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

(h) Bank shall 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).

(i) Bank shall not permit its accounts to be used by shell banks.

## **5. WIRE TRANSFERS**

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

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

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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.

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

The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the

potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, Bank shall ensure that all wire transfers are accompanied by the following information.

**(1) Cross-border wire transfers**

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

(ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

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

**(2) Domestic wire transfers**

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

(ii) If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank shall insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.

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

**(c) Exemptions**

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

**(d) Role of Ordering, Intermediary and Beneficiary Banks**

**(i) Ordering Bank**

An Ordering Bank is the one that originates a wire transfer as per the order placed by its customer. As Ordering Bank, the Bank shall ensure that qualifying wire transfers contain complete originator information. The Bank shall also verify and preserve the information at least for a period of five years.

**(ii) Intermediary Bank**

For both cross-border and domestic wire transfers, Bank processing an intermediary element of a chain of wire transfers shall 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 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.

**(iii) 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. As Beneficiary Bank, the Bank shall 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 Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

## **6. MAINTENANCE OF KYC DOCUMENTS AND PRESERVATION PERIOD**

PML Act and Rules cast certain obligations on the banks with regard to maintenance, preservation and reporting of customer account information. Bank shall take all steps considered necessary to ensure compliance with the requirements of the Act and Rules *ibid*.

### **6.1 Maintenance of records of transactions**

Bank shall have 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), as mentioned below:

- (A) all cash transactions of the value of more than Rupees ten lakh or its equivalent in foreign currency;
- (B) series of all cash transactions integrally connected to each other which have been individually valued below Rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees ten lakh or its equivalent in foreign currency;
- (BA) all transactions involving receipts by non-profit organisations of value more than Rupees ten lakh, or its equivalent in foreign currency;
- (C) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- (D) all suspicious transactions whether or not made in cash and by way of—
  - (i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of—
    - (a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
    - (b) travellers cheques, or
    - (c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
    - (d) any other mode in whatsoever name it is referred to;
  - (ii) credits or debits into or from any non-monetary accounts such as D-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;
  - (iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:—
    - (a) payment orders, or
    - (b) cashiers cheques, or
    - (c) demand drafts, or
    - (d) telegraphic or wire transfers or electronic remittances or transfers, or
    - (e) internet transfers, or
    - (f) Automated

Clearing House remittances, or (g) lock box driven transfers or remittances, or remittances for credit or loading to electronic cards, or (i) any other mode of money transfer by whatsoever name it is called;

(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of— (a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or (b) purchase and negotiation of bills, cheques and other instruments, or (c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or (d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

(v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

(E) 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;

(F) all purchase and sale by any person, of immovable property valued at Rupees fifty lakh or more that is registered by the reporting entity, as the case may be.

Bank shall maintain all necessary information in respect of transactions prescribed under Rule 3 of PML Rules, 2005 so as to permit reconstruction of individual transactions, including the following information:

- (a) the nature of the transactions;
- (b) the amount of the transaction and the currency in which it was denominated;
- (c) the date on which the transaction was conducted; and
- (d) the parties to the transaction.

## **6.2 Preservation of Records**

Bank shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

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

(iii) Bank shall maintain records of the identity of clients, and records in respect of transactions with its clients referred to in Rule 3, in hard or soft format.

(iv) Bank shall 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 shall, as far as possible, be examined and the findings, at branch as well as Principal Officer level, shall be properly recorded. Such records and related documents shall be made available to help auditors to scrutinize the transactions and also to Reserve Bank / other relevant authorities. These records will be preserved for five years as is required under PMLA, 2002.

## **7. COMBATING FINANCING OF TERRORISM (CFT)**

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC):

(a) The ISIL (Da'esh) & Al-Qaida Sanctions List includes names of individuals, groups, undertakings and entities associated with the ISIL (Da'esh) /Al-Qaida. The updated ISIL (Da'esh) /Al-Qaida Sanctions List is available at [http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml).

(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>.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Bank shall take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, as detailed under para 7.1.

Branches are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed customer does not match with that of the UN list of Terrorist individuals/organization/entities, before opening any new account. Branches are also required to cross check the details of all existing accounts with the updated list and ensure that no account is held by or linked to any of the entities or individuals included in the list maintained for this purpose. If the particulars of any of the account/s have resemblance with those appearing in the list, branches have to verify transactions carried out in such accounts and report those accounts to RBI/Financial Intelligence Unit-INDIA, New Delhi.

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

(a) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

(b) Bank shall strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annexure VII to this note) and ensure meticulous compliance to the Order issued by the Government.

## **7.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations**

(a) Bank shall take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the Financial Action Task Force (FATF) Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, Bank shall also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. Bank shall 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) Bank shall 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 shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to Reserve Bank/other relevant authorities, on request.

## **8. REPORTING REQUIREMENTS**

### **(a) Reporting to Financial Intelligence Unit-India**

(i) In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations [NPO means 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 (erstwhile Section 25 of Companies Act, 1956) Section 8 of the Companies Act, 2013], cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

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

(ii) FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website.

(iii) In terms of Rule 8, 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 constitute a separate violation. Branches shall take note of the timeliness of the reporting requirements and submit the reports within the timelines.

As a part of transaction monitoring mechanism, Bank shall put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. The software shall be robust enough to throw the alerts for effective identification and reporting of suspicious transactions.

As per Rule 7 of PML Rules, the procedure and manner of furnishing information shall be as under:

(1) The Bank shall communicate to the Director, FIU IND the name, designation and address of the Designated Director and the Principal Officer.

(2) The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity (details of above clauses are furnished under para 6.1). A copy of such information shall be retained by the Principal Officer for the purposes of official record

(3) The Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in clauses (A),(B),(BA),(C),(D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by its Regulator.

(4) The Bank, its Designated Director, officers and employees shall observe the procedure and the manner of furnishing information as specified by its Regulator.

**(b) Reports to be furnished to FIU-IND:**

**1. Cash Transaction Reports (CTR)**

The Bank shall scrupulously adhere to the following:

(i) The Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. Bank shall ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

(ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer of the Bank to FIU-IND in the specified format (Counterfeit Currency Report- CCR) by 15<sup>th</sup> day of the next month. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

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

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

(v) A summary of cash transaction report for the Bank as a whole shall be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted to FIU-IND. In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under Core Banking Solution at one point for onward transmission to FIU-IND, provided the CTR is generated in the format prescribed by FIU-IND.

(vi) A copy of the monthly CTR submitted to FIU-India in respect of the branches shall be available at the Bank for production to auditors/inspectors, when asked for.

(vii) The instruction on 'Maintenance of records of transactions' and 'Preservation of records' as contained at Para 6 (i) and (ii) respectively shall be scrupulously followed by the branches.

## **2. Suspicious Transaction Reports (STR)**

(i) While determining suspicious transactions, Bank shall be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time.

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

(iii) Bank shall make STRs if there is a reasonable ground to believe that the transaction involve proceeds of crime irrespective of the amount of transaction and / or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

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

(v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, branches may consider the indicative list of suspicious activities contained in Annexure-V of this Note.

(vi) Bank shall not put any restrictions on operations in the accounts where an STR has been filed. Bank and their employees shall keep the fact of furnishing of STR strictly confidential, as required under PML rules. Moreover, it shall be ensured that there is no tipping off to the customer at any level.

The Bank has implemented centralized processing and submission of STRs on the following lines:

1. Circle Offices shall centrally process the alerts pertaining to their branches and escalate suspicious transactions, if any, to KYC Cell, RBS & MIS Wing, HO for review and submission of STRs to FIU-IND, Delhi.
2. The Manager-in-charge of BS&IC Section at Circle would be the Anti Money Laundering Officer (AMLO). The Executive overseeing BS&IC Section would be the Money laundering Reporting Officer (MLRO).
3. KYC Cell, RBS & MIS Wing, HO would review the alerts escalated by the Circles as suspicious transactions and submit STRs wherever required to FIU-IND.

## **3. Non-Profit Organisation (NPO)**

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.

## **4. Cross-border Wire Transfer Report**

Cross-border Wire Transfer Report (CWTR) is required to be filed 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.

As per recent amendments to Prevention of Money Laundering (PML) Rules, every reporting entity is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs.5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India.

The information shall be furnished electronically in the FIN-Net module developed by FIU-IND.

## **9. GENERAL GUIDELINES:**

### **(i) Confidentiality of customer information:**

The information collected from the customer 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 etc. Information sought from the customer shall be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer shall be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

### **(ii) Secrecy Obligations and Sharing of Information:**

Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

While considering the requests for data/ information from Government and other agencies, Bank shall satisfy itself 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:

- a. Where there is a duty to the public to disclose.
- b. The interest of Bank requires disclosure and
- c. Where the disclosure is made with the express or implied consent of the customer.

### **(iii) Avoiding hardship to customers:**

Branches should keep in mind the spirit of instructions issued by the RBI and avoid undue hardships to individuals who are otherwise classified as low risk customers.

### **(iv) Sensitising Customers**

Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. Bank shall, therefore, prepare specific literature / pamphlets etc. to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.

### **(v) Hiring of Employees**

KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank shall put in place adequate screening mechanism as an integral part of its personnel recruitment / hiring process.

#### **(vi) Employee Training**

Bank shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers.

The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Bank, regulation and related issues shall be ensured.

#### **(vii) Accounts under Foreign Contribution Regulation Act, 2010 (FCRA)**

In terms of the Foreign Contribution Regulation Act, 2010, certain categories of individuals and organizations are required to obtain prior permission from the Central Government (Secretary, Ministry of Home Affairs, GOI, New Delhi) to receive “Foreign Contributions” or accept “Foreign Hospitality” and such receipts/acceptance require reporting to the Government.

- Individuals/Organizations who cannot receive foreign contributions : Foreign contributions cannot be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employee of any corporation, member of any legislature, political party or office bearer thereof.
- Individuals/Organizations who can receive foreign contributions: An association having a definite cultural, economic, educational, religious or social programme can receive foreign contribution after it obtains the prior permission of the Central Government or gets itself registered with the Central Government.

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

#### **(viii) Technology requirements:**

The AML software in use at the Bank shall be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold/silver/platinum, payment of dues of credit cards/reloading of prepaid/travel cards, third party products, and transactions involving internal accounts of the Bank.

#### **(ix) Designated Director on the Board of the Bank:**

Bank has nominated the Executive Director overseeing RBS & MIS Wing of the Bank as a Designated Director on the Board of the Bank, as required under the provisions of the PML Rules, 2005, to ensure compliance with the obligations under the Act and Rules. The Designated Director shall oversee the compliance position of AML norms in the Bank.

If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may -

- (a) issue a warning in writing; or
- (b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

- (c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
- (d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

It shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions.

**(x) Principal Officer**

Bank has appointed a Principal Officer. The Principal Officer shall be independent and report directly to the senior management or to the Board of Directors.

Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs 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.

The role and responsibilities of the Principal Officer 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 from time to time.

The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by Non-Profit Organisations of value more than Rupees ten lakh or its equivalent in foreign currency to FIU-IND.

The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.

The Principal Officer under PMLA Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

**(xi) Need for photographs and address confirmation:**

Pass port size/stamp size photograph of the depositors shall be obtained in case of all Current Accounts, SB accounts and Term Deposits.

In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public/private limited companies, HUF, trusts, Limited Liability Partnerships etc., and those of minors, photographs of the authorised signatories should be obtained. Photographs of the student account holders should be attested by the school authorities on the reverse.

In case of change in the authorised signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organisations.

Photograph should be obtained in case of NRI accounts also.

Where the accounts are operated by letters of authority, photographs of the authority holders should be obtained, duly attested by the depositors.

**(xii) Opening of Current Account with non-consortium banks**

In terms of extant guidelines of lending under consortium, a bank which is not a member of a consortium/syndicate, shall not open current account or extend any banking facility without the concurrence of the consortium/syndicate. This shall be scrupulously complied with.

**(xiii) Sale of third party products:**

When Bank sells third party products as agent, the responsibility for ensuring compliance with KYC/AML/CFT regulations lies with the third party. However, to mitigate reputational risk to Bank and to enable a holistic view of a customer's transactions, branches are advised as follows:

(a) Even while selling third party products as agents, branches should verify the identity and address of the walk-in customer.

(b) Branches should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in paragraph 6 above (Maintenance of KYC documents and preservation period).

(c) Bank's AML software will capture, generate and analyse alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers.

d) Sale of third party products by branches as agents to customers, including walk-in customers, for Rs.50,000 and above must be (a) by debit to customer's account or against cheques and (b) obtention & verification of the PAN given by the account based as well as walk-in customers. This instruction would also apply to sale of bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rs. 50,000/- and above.

\*\*\*\*\*

### ANNEXURE- III

**Customer Identification Procedure-Features to be verified and Documents that may be obtained from Customers:**

Features	Documents
<b>Accounts of individuals</b>	
<p>Proof of Identity and Address</p>	<p>Where the client is an individual, he shall submit:-</p> <p><b>(iii) Any Officially Valid Document which contains proof of identity/address</b></p> <p>(iv) The Permanent Account Number (PAN) or Form 60 as defined in the Income Tax Rules, 1962,</p> <p>And such other documents including in respect of the nature of business and financial status of the client as may be required by the Bank.</p> <ul style="list-style-type: none"> <li>• Officially Valid Documents (OVD) are as under:               <ol style="list-style-type: none"> <li>I. Aadhaar Card</li> <li>II. Passport</li> <li>III. Driving License</li> <li>IV. Voter Identity Card issued by Election Commission of India</li> <li>V. Job Card issued by NREGA duly signed by an officer of the State Government</li> <li>VI. Letter issued by the National Population Register containing details of name and address</li> <li>VII. Any other document as notified by the Central Government in consultation with the Regulator.</li> </ol> </li> </ul> <p><b><i>Banks can use physical copy of the Aadhaar card as well as e-Aadhaar, masked Aadhaar and offline electronic Aadhaar xml provided by UIDAI, which are various forms of Aadhaar, as Officially Valid Documents (OVD) for the KYC purpose but without e-KYC based authentication for those customers who do not give a declaration that s/he is desirous of receiving her/his entitled benefits for subsidies welfare schemes funded from the Consolidated Fund of India in her/his account directly.</i></b></p> <p><b><i>(As per UIDAI circular dated 23-10-2018 based on the opinion received from the Ld. Attorney General for India after the Aadhaar Judgment of the Hon. Supreme Court of India, delivered on 26-09-2018).</i></b></p>

Accounts of companies	
	<p>Where the client is a company, certified copies of following documents are to be submitted:</p> <ul style="list-style-type: none"> <li>(i) Certificate of incorporation</li> <li>(ii) Memorandum and Articles of Association</li> <li>(iii) A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf.</li> <li>(iv) (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf</i></b> and  (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to managers, officers or employees holding an attorney to transact on the company's behalf.</li> </ul>
Accounts of partnership firms	
	<p>Where the client is a partnership firm, certified copies of following documents are to be submitted:</p> <ul style="list-style-type: none"> <li>(i) Registration Certificate</li> <li>(ii) Partnership Deed</li> <li>(iii) (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf</i></b> and  (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the partnership firm.</li> </ul>
Accounts of trusts	
	<p>Where the client is a Trust, certified copies of following documents are to be submitted:</p> <ul style="list-style-type: none"> <li>(i) Registration Certificate</li> <li>(ii) Trust Deed</li> <li>(iii) (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf</i></b> and  (b) PANs or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the Trust.</li> </ul>

<b>Accounts of Unincorporated Association or body of individuals</b>	
	<p>Where the client is an unincorporated association or a body of individuals, certified copies of following documents are to be submitted:</p> <ul style="list-style-type: none"> <li>(i) Resolution of the managing body of such association or body of individuals</li> <li>(ii) Power of Attorney granted to the person who will transact on its behalf.</li> <li>(iii) (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf</i></b> and (b) <b><i>PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the unincorporated association or a body of individuals.</i></b></li> </ul>
<b>Accounts of Government or its Departments, Societies, Universities and Local Bodies like Village Panchayats.</b>	
	<ul style="list-style-type: none"> <li>i. Document showing name of the person authorized to act on behalf of the entity;</li> <li>ii. (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf</i></b> and (b) <b><i>PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf.</i></b></li> </ul>
<b>Accounts of Proprietorship Concerns</b>	
Proof of name, address and activity of the concern	<p>For Proprietary concerns, in addition to the <b>PAN No.</b> and <b>Officially Valid Documents</b> applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern should be submitted:</p> <ul style="list-style-type: none"> <li>a) Registration Certificate (in the case of a registered concern).</li> <li>b) Certificate / licence issued by the Municipal authorities under Shop &amp; Establishment Act.</li> <li>c) Sales and income tax returns.</li> <li>d) CST / VAT certificate.</li> <li>e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.</li> <li>f) Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.</li> <li>g) The complete Income Tax return (not just the acknowledgement) in the name of the sole</li> </ul>

		<p>Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities.</p> <p>h) Utility bills such as electricity, water and landline telephone bills.</p> <p>i) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.</p> <p>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 branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, 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.</p>
--	--	---

**Accounts of Limited Liability Partnerships**

	<p>Proof of name, address and activity of the concern</p>	<p>(i) Certified copy of incorporation documents filed with Registrar of Companies.</p> <p>(ii) Certificate issued by the Registrar of Companies.</p> <p>(iii) Copy of LLP Agreement signed by all the partners. In case, there is no LLP agreement, Schedule I of the LLP Act signed by all the partners will prevail.</p> <p>(iv) (a) <b><i>Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf and</i></b>  (b) PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf.</p>
--	---	--

**Relaxation for Accounts of low risk customers**

<p>'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the</p>	<p>Additional documents deemed to be OVDs for the purpose of proof of identity where simplified measures are applied:</p> <p>(i) identity card with applicant's Photograph issued by Central/ State Government Departments, Statutory/ Regulatory</p>
--	---

<p>overall money laundering and terrorist financing risks involved.</p>	<p>Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;</p> <p>(ii) letter issued by a gazetted officer, with a duly attested photograph of the person.</p> <p>For the limited purpose of proof of address, the following additional documents are deemed to be OVDs where simplified measures are applied:</p> <p>(a) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);</p> <p>(b) Property or Municipal Tax receipt;</p> <p>(c) Bank account or Post Office savings bank account statement;</p> <p>(d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;</p> <p>(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</p> <p>(f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.</p>
<p>Branches to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.</p>	

## ANNEXURE- IV

### List of Low/Medium/High risk Customers based on the recommendations of IBA Working Group.

#### APPENDIX - A

Low Risk	Medium Risk	High Risk
<ol style="list-style-type: none"> <li>1. Cooperative Bank</li> <li>2. Ex-staff, Govt./ Semi Govt. Employees</li> <li>3. Illiterate</li> <li>4. Individual</li> <li>5. Local Authority</li> <li>6. Other Banks</li> <li>7. Pensioner</li> <li>8. Public Ltd.</li> <li>9. Public Sector</li> <li>10. Public Sector Bank</li> <li>11. Staff</li> <li>12. Regional Rural Banks</li> <li>13. Govt./Semi-Govt. Local Body</li> <li>14. Senior Citizens</li> <li>15. Self Help Groups</li> </ol>	<ol style="list-style-type: none"> <li>1. Gas Station</li> <li>2. Car / Boat / Plane Dealership</li> <li>3. Electronics (wholesale)</li> <li>4. Travel agency</li> <li>5. Used car sales</li> <li>6. Telemarketers</li> <li>7. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center</li> <li>8. Dot-com company or internet business</li> <li>9. Pawnshops</li> <li>10. Auctioneers</li> <li>11. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.</li> <li>12. Sole Practitioners or Law Firms (small, little known)</li> <li>13. Notaries (small, little known)</li> <li>14. Secretarial Firms (small, little known)</li> <li>15. Accountants (small, little known firms)</li> <li>16. Venture capital companies</li> <li>17. Blind</li> <li>18. Purdanashin</li> <li>19. Registered Body</li> <li>20. Corporate Body</li> <li>21. Joint Sector</li> <li>22. Partnership</li> </ol>	<ol style="list-style-type: none"> <li>1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.</li> <li>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</li> <li>3. Individuals and entities in watch lists issued by Interpol and other similar international organizations</li> <li>4. Customers with dubious reputation as per public information available or commercially available watch lists</li> <li>5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk</li> <li>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.</li> <li>7. Customers based in high risk countries/jurisdictions or locations (refer <b>Appendix C</b>)</li> <li>8. Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;</li> <li>9. Non-resident Customers</li> <li>10. Embassies / Consulates</li> <li>11. Off-shore (foreign) corporation/ business</li> </ol>

	<p>23. Private Bank  24. Private Limited Company  25. Unregistered body  26. Proprietorship</p>	<p>12. Non face-to-face Customers  13. High net worth individuals  14. Firms with 'sleeping partners'  15. Companies having close family shareholding or beneficial ownership  16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale  17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence  18. Investment Management / Money Management Company/Personal Investment Company  19. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.  20. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)  21. Money Service Business: including seller of: Money Orders / Travelers' Cheques / Money Transmission / Cheque Cashing / Currency Dealing or Exchange  22. Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques/cash payroll cheques)  23. Gambling/gaming including "Junket Operators" arranging gambling tours  24. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)</p>
--	---	--

		<ul style="list-style-type: none"> <li>25. Customers engaged in a business which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries)</li> <li>26. Customers engaged in industries that might relate to nuclear proliferation activities or explosives</li> <li>27. Customers that may appear to be Multi level marketing companies etc.</li> <li>28. Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence)</li> <li>29. Associations/Clubs</li> <li>30. Foreign Nationals</li> <li>31. NGO</li> <li>32. Overseas Corporate Bodies</li> <li>33. Bullion dealers and Jewelers (subject to enhanced due diligence)</li> <li>34. Pooled accounts</li> <li>35. Other Cash Intensive business</li> <li>36. Shell Banks - Transactions in corresponding banking</li> <li>37. Non-Bank Financial Institution</li> <li>38. Stock brokerage</li> <li>39. Import / Export</li> <li>40. Executors/Administrators</li> <li>41. HUF</li> <li>42. Minor</li> <li>43. Accounts under Foreign Contribution Regulation Act</li> </ul>
--	--	---

**The above categorization of customers under risk perception is only illustrative and not exhaustive.**

## **APPENDIX - B**

### **High / Medium Risk Products and Services**

Branches / Offices are required to pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Presently a variety of Electronic Cards are used by customers for buying goods and services, drawing cash from ATMs, and for electronic transfer of funds. Branches should ensure that appropriate KYC procedures are duly applied before issuing the Cards including Add-on / Supplementary Cards to the customers.

### **Indicative list of High / Medium Risk Products and Services**

1. Electronic funds payment services such as Electronic cash (e.g., stored value and pay roll cards), funds transfer (domestic and international) etc.
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6. Foreign correspondent accounts
7. Trade finance (such as letters of credit)
8. Special use or concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities
10. Non-deposit account services such as Non-deposit investment products and Insurance
11. Transactions undertaken for non-account holders (occasional Customers)
12. Provision of safe custody and safety deposit boxes
13. Currency exchange transactions
14. Project financing of sensitive industries in high-risk jurisdictions
15. Trade finance services and transactions involving high-risk jurisdictions
16. Services offering anonymity or involving third parties
17. Services involving banknote and precious metal trading and delivery
18. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

## APPENDIX - C

### High / Medium Geographic risk

Branches/offices are required to prepare a profile for all new customers based on risk categorization, taking into account the location of the customer and the customer's clients as well as factors such as the nature of business activity, mode of payments, turnover and customer's social and financial status including location of his business activity and to exercise due diligence based on the bank's risk perception.

The customer should be subjected to higher due diligence if following criteria falls under "high-risk" geographies

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

Apart from the risk categorization of the countries, branches/offices should categorize the geographies/locations within the country on both Money Laundering (ML) and Financing Terrorism (FT) risk.

### Indicative List of High / Medium Risk Geographies

#### Countries/Jurisdictions

1. Countries subject to sanctions, embargos or similar measures in the United Nations Security Council Resolutions ("UNSCR").
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks ([www.fatf-gafi.org](http://www.fatf-gafi.org))
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies ([www.fatf-gafi.org](http://www.fatf-gafi.org))
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
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 organisations operating within them.
7. Countries identified by credible sources as having significant levels of criminal activity.
8. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

**Locations**

1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations/cities and affected districts)
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.

**NOTE:**

Risk assessment should take into account following risk variables specific to a particular customer or transaction:

- The purpose of an account or relationship
- Level of assets to be deposited by a particular customer or the size of transaction undertaken.
- Level of regulation or other oversight or governance regime to which a customer is subjected to.
- The regularity or duration of the relationship.
- Familiarity with a country, including knowledge of local laws, regulations and rules as well as structure and extent of regulatory oversight.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or increase the complexity or otherwise result in lack of transparency.

## ANNEXURE-V

### **Monitoring of Customer Risk Categorisation (CRC):**

Customer Behaviour Indicators which may lead to migration of Risk categorization to “High Risk” are as follows:

- Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the Bank to verify.
- Customer expressing unusual curiosity about secrecy of information involved in the transaction.
- Customers who decline to provide information that in normal circumstance would make the customers eligible for banking services.
- Customer giving confusing details about a transaction.
- Customer reluctant or refuses to state a purpose of a particular large/ complex transaction/source of funds involved or provides a questionable purpose and / or source.
- Customers who use separate tellers to conduct cash transactions or foreign exchange transactions.
- Customers who deposit cash/ withdrawals by means of numerous deposit slips/ cheques leaves so that the total of each deposits is unremarkable, but the total of all credits/ debits is significant.
- Customer’s representatives avoiding contact with the branch.
- Customer who repays the problem loans unexpectedly.
- Customers who appear to have accounts with several banks within the same locality without any apparent logical reason.
- Customer seeks to change or cancel a transaction after the customer is informed of currency transaction reporting/ information verification or record keeping requirements relevant to the transaction.
- Customers regularly issue large value cheques without balance and then deposits cash.
- Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

### **Transactions involving large amounts of cash:**

- Exchanging an unusually large amount of small denomination notes for those of higher denomination.
- Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.
- Frequent withdrawal of large amounts by means of cheques, including traveler’s cheques.
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer’s business activity.
- Large cash withdrawals from a previously dormant/ inactive account, or from an account which has just received an unexpected large credit from abroad.

- Company transactions, both deposits and withdrawals that are denominated by unusually large amounts of cash rather than by way of debits and credits normally associated with the normal commercial operations of the company e.g. cheques , letters of credit , bills of exchange etc.
- Depositing cash by means of numerous credit slips by a customer, such that the amount of each deposit is not substantial, but the total of which is substantial.

**Transactions that do not make Economic Sense:**

- Customer having multiple accounts with the bank, with frequent transfers between different accounts.
- Transactions in which amounts are withdrawn immediately after being deposited, unless the customer's business activities furnish plausible reasons for immediate withdrawal.

**Activities not consistent with the customer's business:**

- Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
- Corporate accounts where deposits and withdrawals by cheque / telegraphic transfers/ foreign inward remittances/ any other means are received from / made to sources apparently unconnected with the corporate business activity/ dealings.
- Unusual applications for DD/ PO/NEFT/RTGS against cash.
- Accounts with large volume of credits through DD/ PO/NEFT/RTGS whereas the nature of business does not justify such credits.
- Retail deposit of many cheques but rare withdrawals for daily operations.

**Attempts to avoid reporting/ record- keep requirements:**

- A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- Any individual or group that coerces/ induces or attempts to coerce/ induce a bank employee not to file any reports or any other forms.
- An account where there are several cash deposits /withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customers intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

**Unusual Activities**

- An account of a customer who does not reside / have office near the branch even though there are bank branches near his residence/ office.
- A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
- Funds coming from the list of countries / centres, which are known for money laundering.

**Customer who provides insufficient or suspicious information**

- A customer / company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors or its locations.
- A customer / company who is reluctant to reveal details about his/its activities or to provide financial statements.
- A customer who has no record of past or present employment but makes frequent large transactions.

**Certain suspicious funds transfer activities:**

- Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- Receiving large DD/ NEFT/ RTGS remittances from various centres and remitting the consolidated amount to a different account / centre on the same day leaving a minimum balance in the account.
- Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire / fund transfer.

## Annexure- VII

### Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

1. In respect of funds, financial assets or economic resources or related services held in the form of bank accounts, the RBI would forward the designated lists to the banks. The RBI would issue necessary guidelines to banks, requiring them to:-

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Govt. Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(iii) The banks shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(v) The banks shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

2. On receipt of the particulars referred to in para 1 (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

3. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be

engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act. The order shall take place without prior notice to the designated individuals/entities.

**Regarding financial assets or economic resources of the nature of immovable properties.**

4. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

5. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

6. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail.

7. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail. MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

8. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT. The order shall take place without prior notice, to the designated individuals/entities.

9. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to 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. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

10. 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 owned 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. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

11. 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.

12. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 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 Regulators, FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

13. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 1 to 9 above shall be followed. The freezing orders shall take place without prior notice to the designated persons involved.

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

14. 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, Registrar of Immovable Properties and the State/UT nodal officers.

15. The banks, Registrar of Immovable Properties and the State/UT nodal officers 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 as per the contact details given in paragraph 1(ii) above within two working days.

16. 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 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. 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.**

17. 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 banks through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

**Regarding prevention of entry into or transit through India**

18. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

19. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

**Procedure for communication of compliance of action taken under Section 51A.**

20. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

\*\*\*\*\*