THE ZOROASTRIAN CO-OPERATIVE BANK LIMITED

KYC/ AML POLICY

2019-20

INDEX

Introduction

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

I. General Guidelines

i. The information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. The Bank will ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer will be sought separately with his/her consent and after opening the account.

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

II. Key elements of the KYC Policy

1.Customer Acceptance Policy;

2.Customer Identification Procedures

3.Monitoring of Transactions; and

4.Risk Management.

1. Customer Acceptance Policy (CAP)

The Customer Acceptance Policy will ensure that explicit guidelines are in place on the following aspects of customer relationship in the Bank.

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

ii. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (The Bank may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) will be categorised under high risk category.

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

iv. The Bank will not open an account or close an existing account where the Bank is unable to apply appropriate customer due diligence measures, i.e., Bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-co-operation of the customer or non reliability of the data/information furnished to the Bank. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by the Bank to close an account will be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

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

vi. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.

vii. The Bank will prepare a profile for each new customer based on risk categorization and the customer profile will contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. However, while preparing customer profile the Bank will take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein will not be divulged for cross selling or any other purposes.

viii. For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the Bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc.

ix. The Bank will obtain Permanent Account Number of (PAN) of all customers and verify at the time of account opening as per the provisions of Income Tax Act, (Rule 114 B) applicable to Banks and amended from time to time.

The Bank applies enhanced due diligence measures based on the risk assessment, thereby requiring intensive ‘due diligence’ for higher risk customers, especially those for whom the sources of funds are not clear. In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewelers will also be categorized by the Bank as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; (g) non-face to face customers and (h) those with dubious reputation as per public information available etc. However, only NPOs/NGOs promoted by United Nations or its agencies will be classified as low risk customers.

x. In addition to what has been indicated above, the Bank will take steps to identify and assess their risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels, to effectively manage and mitigate their risk adopting a risk-based approach. In this regard, the Bank for guidance in its own risk assessment, will adhere to a Report on Parameters for Risk-Based Transaction Monitoring (RBTM) dated March 30, 2011 issued by Indian Banks' Association on May 18, 2011 as a supplement to its guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009.

xi. The Bank will ensure that the adoption of customer acceptance policy and its implementation is not too restrictive and must not result in denial of Banking services to general public, especially to those, who are financially or socially disadvantaged.

2. **Customer Identification Procedure (CIP)**

i. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. The Bank shall obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of Banking relationship. The Bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to Banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the Bank will obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Bank will (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons require an extra element of caution and is enumerated under paragraph 2.5 below.

The Bank will accept such accounts in terms of the Customer Acceptance Policy. The Bank will take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are [Ref: Government of India Notification dated June 16, 2010 - Rule 9 sub-rule (1A) of PML Rules].

ii. The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a Bank, across the Banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer.

The Unique Customer Identification Code (UCIC) is allotted by the Bank to all its customers. The said facility will help 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. It would also smoothen Banking operations for the customers.

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

iv When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, the Bank shall review the due diligence measures including re-verifying the identity of the client and obtaining information on the purpose and intended nature of the business relationship. [Ref: Government of India Notification dated June 16, 2010-Rule 9 sub-rule (1D) of PML Rules].

v It has been observed that some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some Banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, the Bank will obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. The Bank can use any supplementary evidence such as a letter received through post for further verification of the address.

While issuing operational instructions to the branches on the subject, the Bank shall keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

vi KYC once done by one branch of the Bank will be valid for transfer of the account within the Bank as long as full KYC has been done for the concerned account. The customer will be allowed to transfer his account from one branch to another branch without restrictions. In order to comply with KYC requirements of correct address of the person, fresh address proof will be obtained from him/her upon such transfer by the transferee branch.

vii The Bank has initiated a system of periodical updation of customer identification data (obtaining KYC documents) after the account is opened. The periodicity of such updation is once in 10 years in case of low risk category customers, once in eight years in case of medium risk categories and once in two years in case of high risk customers. Such verification will be done irrespective of whether the account has been transferred from one branch to another.

viii The Bank's Account Opening Form is enclosed by way of **Annexure-I.** An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure-II**. It is clarified that the communication address, as referred to in Annexure-I, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the Bank for verification of the address of the customer.

ix The Bank will obtain proof of Income of its customers other than Minors and Housewife failing which the account will directly be classified under medium risk. Further, the Branch Managers will verify all the KYC documents, authenticate them and forward the same to the Centralised Account Opening Team at Back Office. Thereafter, the concerned official at the Account Opening Cell will verify the KYC documents, PAN from the Income Tax portal and accordingly authenticate the documents as Verified.

x. In line with the latest judgement of the Supreme Court on Aadhaar, acceptance of Aadhaar is not mandatory as a part of KYC document before opening new accounts.

2. Customer Identification Requirements – Indicative Guidelines

i) Walk-in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address will 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.50,000/- the Bank will verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

NOTE: In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 Banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

ii) Salaried Employees

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

iii) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The Bank will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the Bank will insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a Trust, the Bank will take reasonable precautions to verify the identity of the Trustees and the settlors of Trust (including any person settling assets into the Trust), guarantors, protectors, beneficiaries and signatories. The Beneficiaries will be identified when they are defined. In the case of a 'foundation', the Bank will take steps to verify the founder managers/ directors and the beneficiaries, if defined.

iv) **Accounts of Companies and Firms**

The Bank will be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Bank. The Bank will 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.

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

a) When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. The Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. The Bank will also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the Bank, the Bank will look through to the beneficial owners. Where the Bank will rely on the 'Customer Due Diligence' (CDD) done by an intermediary, the Bank will satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

b) Under the extant Anti-Money Laundering / Combating the Financing of Terrorism framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that the Banks will not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality.

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

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

a) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Bank will gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. The Bank will verify the identity of the person and seek information about the sources of funds before accepting the Politically Exposed Persons as a customer.

The decision to open an account for a PEP will be taken at a senior level in the Bank which will be clearly spelt out in Customer Acceptance Policy. The Bank will also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

b) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, the Bank will obtain approval of the Board of Directors to continue the business relationship. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

c) Further, the Bank shall monitor ongoing risk management procedures for identifying PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

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

In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, the Bank will adhere to specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented will be insisted upon and, if necessary, additional documents may be called for. In such cases, the Bank may also require the first payment to be effected through the customer's account with another Bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the Bank may have to rely on third party certification/introduction. In such cases, the Bank will ensure that the third party is a regulated and supervised entity and has adequate KYC systems in place.

viii) **Accounts of proprietary concerns**

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, the Bank will call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT/GST certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. The Bank may also accept IEC (Importer Exporter Code) issued to the proprietary concern, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

ix) **Accounts with Introduction**

a. Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, 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 such documents 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.

Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annexure-I of this master circular, the Banks should open an account for him, subject to: Introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the Bank should be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account as also his address need to be certified by the introducer, or any other evidence as to the identity and address of the customer to the satisfaction of the Bank.

b. While opening accounts as described above, the customer will be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the Bank will notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

x) **Small Accounts**

a) 'Small Account' means a savings account in a Banking company where-

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

(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

(iii) the balance at any point of time does not exceed rupees fifty thousand .

The Bank will ensure adherence to the procedure provided in the Rules for opening of small accounts.

b) Officially Valid Documents

a. 'Officially Valid Document' as contained in clause (d) of Rule 2(1)of the PML Rules includes job card issued by NREGA (National Rural Employment Guarantee Act) duly signed by an officer of the State Government and the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

b. It is further advised that where the Bank has relied exclusively on the NREGA job card as complete KYC document for opening of an account, the Bank account so opened will also be subjected to all conditions and limitations prescribed for 'small account' as mentioned earlier.

c. While opening accounts based on Aadhaar, the Bank will satisfy the correct address of the customer by obtaining required proof of the same as per extant instructions.

Customer Identification Procedure is brought out by way of **Annexure-III**.

xi) **Operation of Bank Accounts & Money Mules**

a) "Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.
b) In a money mule transaction, an individual with a Bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their Bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a time the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

xii) **Bank No Longer Knows the True Identity**

In the circumstances when the Bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the Bank will file a Suspicious Transaction Report (STR) with FIU-IND.

3. **Monitoring of Transactions**

a) Ongoing monitoring is an essential element of effective KYC procedures. The Bank will control and reduce its risk by understanding of the normal and reasonable activity of the customer so as to identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account.

The Bank will monitor unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The Bank will prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Currently the threshold limit placed is Rs 2 lakhs and above. The Bank will thoroughly monitor transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts will be subjected to intensified monitoring.

b) The Bank will 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 will be carried out at yearly intervals.

c) The Bank will exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds [Ref: Government of India Notification dated June 16, 2010 -Rule 9, sub-rule (1B)]

d) The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by the Bank will be effectively carried out for proper implementation of KYC/AML/CFT measures. The Bank will continue the process of risk categorization and compiling/updating profiles of all of their existing customers at a periodicity of once in six months.

Closure of accounts - Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-co-operation by the customer, the Bank will consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions will be be taken at a reasonably senior level.

4. **Risk Management**

a) The Bank will adhere to the above points and follow appropriate procedures in ensuring effective implementation of KYC/AML. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters.

The Bank has Senior Level Personnel appointed as a Principal Officer for ensuring that the Bank's policies and procedures are implemented effectively ensuring proper procedures for creating risk profiles of their existing and new customers, assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc.

b).The Bank will ensure that its audit machinery is staffed adequately with individuals who are well-versed in KYC/AML policies and procedures. Concurrent/ Internal Auditors have been specifically informed to check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard will be placed before the Audit Committee of the Board of Directors at quarterly intervals.

III. Issue and Payment of Demand Drafts

The Bank will ensure that any remittance of funds by way of demand draft, NEFT or any other mode for value of Rs 20,000/- and above will be effected by debit to the customers account only and not cash payment. The Bank shall not issue any demand draft/pay orders or conduct any electronic transactions for walk-in-customers against cash payment.

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

IV. Combating Financing of Terrorism

a) In terms of PMLA Rules, suspicious transaction include, *inter alia,* transactions, which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. The Bank will continue to carry out enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-IND on priority.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all Banks and financial institutions. The Bank will periodically update the lists of individuals and entities as circulated by Reserve Bank of India. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

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

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

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

The Bank ensures that before opening any new account the name/s of the proposed customer does not appear in the lists as mentioned above. Further, the Bank scans all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list will be immediately intimated to RBI and FIU-IND.

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

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

ii. The Bank is required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009, **Annexure-IV** and ensure meticulous compliance to the Order issued by the Government.

iii. On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, the Bank will ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of Bank accounts.

iv. In regard to 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 requiring them to:

a) 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 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.

b) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the Bank 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 will necessarily be conveyed on e-mail.

c) The Bank shall also send by post a copy of the communication mentioned in (b) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Central Office, Reserve Bank of India, Anti Money Laundering Division, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai - 400 001 and also by fax at No.022-22701239. The particulars apart from being sent by post/fax will necessarily be conveyed on e-mail.

d) The Bank will also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the state/UT where the account is held as the case may be and to FIU-India.

e) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the Bank 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 will necessarily be conveyed on e-mail.

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

v. Freezing of financial assets

a) On receipt of the particulars as mentioned in paragraph iv(b) 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.

b) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned Bank's branch under intimation to Reserve Bank of India and FIU-IND.

c) The order shall take place without prior notice to the designated individuals/entities.

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

a) U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

b) 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.

c) The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds,

or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

d) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to Banks.

e) The freezing orders shall take place without prior notice to the designated persons involved.

vii. 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.

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned Bank. The Bank 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 (iv)(b) above within two working days.

The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the Bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

viii. Communication of Orders under section 51A of Unlawful Activities (Prevention) Act. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to the Bank through RBI.

VI. Correspondent Banking

Correspondent Banking is the provision of Banking services by one Bank (the "correspondent Bank") to another Bank (the "respondent Bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. The Bank will gather sufficient information to understand fully the nature of the business of the correspondent/respondent Bank. Information on the other Bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent Banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, the Bank will ascertain from publicly available information whether the other Bank has been subject to any money laundering or terrorist financing investigation or regulatory action.

While it is desirable that such relationships should be established only with the approval of the Board of Directors, they may delegate the power to a committee headed by the Chairman/CEO of the Bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee will be invariably placed before the Board of Directors at its meeting for post facto approval. The responsibilities of the Bank with whom correspondent Banking relationship is established will be clearly documented. In the case of payable-through-accounts, the correspondent Bank should be satisfied that the respondent Bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent Bank should also ensure that the respondent Bank is able to provide the relevant customer identification data immediately on request.

VII. Correspondent relationship with a "Shell Bank"

The Bank will 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).

VIII. Principal Officer

a) In terms with RBI guidelines, the Bank has a Senior Level Personnel appointed as a Principal Officer for KYC/AML. The Principal Officer will act independently and report directly to the Board of Directors. Principal Officer shall be located at the head/corporate office of the Bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, Banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism

b) Further, the role and responsibilities of the Principal Officer will 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 will also be 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.

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

The Amendments to the prevention of Money Laundering Act is enclosed by way of **Annexure-V**.

IX. Designated Director:

In line with RBI guidelines, a Designated Director is appointed by the Board of Directors. The Bank has nominated a Designated Director and the name, designation and address of the Designated Director is communicated to the FIU-IND.

X. Maintenance of records of transactions

The Bank should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of 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. all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;
c. all transactions involving receipts by Non-Profit organisations of value more than Rupees Ten Lakhs or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]
d. all cash transactions where forged or counterfeit currency notes or Bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and

e. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

The Bank will maintain all necessary information 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

XI. Maintenance and Preservation of Records

a) All records containing information of all transactions including the records of transactions as detailed above are required to be maintained. The Bank will ensure 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. Further, the Bank will maintain for at least ten 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.

b) The Bank will ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like aadhar, 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 ten years after the business relationship is ended as required under Rule 10 of the Rules *ibid***.** The identification records and transaction data will be made available to the competent authorities upon request.

XII. Reporting to Financial Intelligence Unit - India

a) In terms of the PMLA Rules, the Bank will report information relating to cash and suspicious transactions and all transactions involving receipts by Non-Profit organisations of value more than Rupees Ten Lakhs or its equivalent in foreign currency through electronic medium to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to Website - http://fiuindia.gov.in/

XIII. Cash and Suspicious Transaction Reports

a) Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the Bank shall scrupulously adhere to the following:

i) The Cash Transaction Report (CTR) for each month will be submitted by the Bank to FIU-IND by 15th of the succeeding month.

ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine will be reported by the Principal Officer to FIU-IND in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency Report – CCR). These cash transactions will 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 should contain only the transactions carried out by the Bank on behalf of their clients/customers excluding transactions between the internal accounts of the Bank.

v) A summary of Cash Transaction Report for the Bank as a whole should be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

XIV. Suspicious Transaction Reports (STR)

i) While determining suspicious transactions, the Bank should be guided by definition of suspicious transaction 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. It is clarified that the Bank on not receiving clear information towards attempted transactions in STRs, contrary to the nature and purpose of business of customers, irrespective of the amount of the transaction will be reported as Suspicious Transaction.

iii) The Bank will report STRs if it has reasonable ground to believe that the transaction involved proceeds of crime generally 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) will 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 will record his reasons for treating any transaction or a series of transactions as suspicious will 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 will 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, the Bank will consider the indicative list of such suspicious activities for reporting to FIU-IND.

vi) The Bank will not place any restrictions on operations in the accounts where an STR has been made.The Bank and its employees will keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It will be ensured that there is no tipping off to the customer at any level.

XV. Non-Profit Organisation

The report of all transactions involving receipts by Non- Profit organizations of value more than Rupees Ten Lakhs 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.

XVI. Customer Education/Employees Training/Employees Hiring

a) Customer Education

Implementation of KYC procedures requires the Bank to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Bank by way of specific literature, display on website etc. educate the customers of the objectives of the KYC/AML. The front desk staff will be specially trained to handle KYC/AML queries while dealing with customers.

b) Employees' Training

The Bank conducts frequent trainings for frontline staff, compliance staff and staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

c) Hiring of Employees

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

XVII. Central KYC Records Registry

The Government vide notification dated 7th July 2015, amended the Prevention of Money Laundering Rules 2005 for setting up of Central KYC Records of customers (Individuals only).

In line with the notification, the Bank is storing and scanning the KYC data of Individual customers to CKYCR in digital form.

XVIII. Customer Compensation

Reserve Bank of India's circular dated 14th December, 2017 highlights liability of the customer pertaining to un-authorised electronic transactions. The detailed guidelines with respect to the circular is brought out in the Bank's Customer Compensation Policy for Financial Year 2019-20. The Bank has already educated its counter staff on the same for customer education and awareness. The said Policy is also placed on the Branch's prominent Notice Boards as well as displayed on the Bank's Website.