



**The Goa Urban Co-operative Bank Ltd.**  
(Registered Office : Dr. Atmaram Borkar Road, Panaji-Goa, 403 001)  
**SCHEDULED BANK**

# **KNOW YOUR CUSTOMER (KYC)/ ANTI MONEY LAUNDERING (AML) POLICY**

**Recommended for  
Approval of BOD in  
BOM meeting dated :**

**12<sup>th</sup> June 2024**

**Approved in the BOD  
meeting dated :**

**12<sup>th</sup> June 2024**



**The Goa Urban Co-operative Bank Ltd.**  
(Registered Office : Dr. Atmaram Borkar Road, Panaji-Goa, 403 001)  
**SCHEDULED BANK**

**Know Your Customer(KYC)/ Anti-Money Laundering (AML) POLICY**

**OBJECTIVE**

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. Branches should ensure that any remittance of funds by way of demand draft, mail/ telegraphic transfer or any mode of funds transfer for a value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheque's and not against cash payment.

iii. Bank shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, bank shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

iv. Bank shall seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and will provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, it shall also be considered to adopt best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better (Whenever/ wherever applicable).

**II. Definition of Customer :**

"Customer" may be defined as :

A person or entity that maintains an account and/ or has a business relationship with the bank.

One on whose behalf the account is maintained (i.e. Beneficial Owner)

Beneficiaries of transactions conducted by professional intermediaries, such as Stock Broker, Chartered Accountants, Solicitors etc., as permitted under the law.

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

### III. 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. An indicative list of customers based on recommendation of IBA is enclosed in **Annexure – II**. The list enclosed is only illustrative and not exhaustive.

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 terrorist or terrorist organisations etc found in the negative list circulated by The Reserve Bank of India.

vii. The increasing complexity and volume of financial transactions necessitate that the customers do not have multiple identities within a bank. The bank will allot a Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships for individual customers. Similarly, existing individual customers should be allotted unique customer identification code. The UCIC will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers.

viii. 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 client's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, 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. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

ix. 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, small businessmen, self employed, 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.

The Bank will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive "due diligence" for higher risk customers, especially those for whom the sources of funds are not clear. In view of the risks involved in cash intensive businesses, accounts of forex & bullion dealers may be categorized by the Bank as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include (a) non-resident customers; (b) high net worth individuals; (c) trusts, charities, NGOs/NPOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs), 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.

x. 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.

xi. Customer Due Diligence (CDD)” shall include identifying and verifying the customer and the beneficial owner using a Risk based approach in regards to ML/TF risks identified, size of business and reliable and independent sources of identification.

The CDD, will be performed at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations and shall include:

- a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
- b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
- c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

Bank may consider filling an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to its customer.

## **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 (a) verify the legal status of the legal person/entity through proper and relevant documents; (b) 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; (c) 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.

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.

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.

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 after verifying 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 deposit account/s 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 Risk-based 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 category customer 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.

## 1. Individual Customers:

- a. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter/self declaration form etc. (Draft format of letter RKYC-IND to be obtained from Individual customer is attached)
- b. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of the bank), letter/Self declaration Form etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.  
Further, bank, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation, in which case verification of address may not be mandatory.
- c. **Accounts of customers who were minor at the time of opening account on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that

CDD documents as per the current CDD standards are available with the bank. Wherever required, bank may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major. Fresh account opening form to be obtained which should be attached to old account opening form with “**MINOR ATTAINS MAJORITY**” words inscribed on the form in **RED INK**. Fresh specimen card to be obtained, duly countersigned by the guardian.

## **2. Customers other than individuals:**

- a. **No change in KYC information:** In case of no change in the KYC information of the Legal Entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of the bank), letter from an official authorized by the LE in this regard, board resolution etc. Further, bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- b. **Change in KYC information:** In case of change in KYC information, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

## **3. Additional measures:** In addition to the above, bank shall ensure that -

- a. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- b. Customer's PAN details, if available with the bank, is verified from the database of the issuing authority (Wherever applicable).
- c. An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- d. Bank shall insist on new photograph of the customer once in 10 years or if there is a relative change in the facial appearance of the customer.
- e. Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at REs' end.

viii An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure-I**. It is clarified that the communication address, 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 declaration of Income of its customer other than Minors and Housewife. Further, the Branch Managers / officers will verify all the KYC documents, authenticate them and forward the same for Opening the account.

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.

## **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. Further, in addition to the certificate/letter issued by the employer, the Bank will insist on at least one of the officially valid documents (OVD) 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 settlers of Trust (including any person settling assets into the Trust), grantors, 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**



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.

Under the extant Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) framework, 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)

Politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and 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/wealth, before accepting the Politically Exposed Persons as a customer.

The decision to open an account for a PEP will be taken by Head of the Branch/ Branch Manager as per the 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.

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

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

Non-face-to-face onboarding facilitates the bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this

Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by bank for nonface-to-face customer onboarding whenever introduced:

a) In case bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP as per RBI guidelines.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Bank shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

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 including Udyam Registration Certificate (URC) issued by the Government, 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. In cases where the branch manager/ officer is satisfied that it is not possible to

furnish two such documents, bank may obtain only one of above document as proof of business/ activity provided branch manager/ officer shall undertake personal contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

ix) Introduction not Mandatory for Opening of Accounts.

Before implementation of the system of document based verification of identity, as laid down in the PML Act/ Rules, introduction from the existing customer of the bank was considered necessary for opening of bank accounts.

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**, 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.

c. Customer submitting required documents of identity and address, as necessary for opening of accounts under PML Act and Rules and/or Reserve Bank's extant KYC guidelines, bank will not insist on introduction for opening of account.

x) Small Accounts

a) 'Small Account' means a savings account opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005 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.

#### 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.

c) Bank shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. If it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the concerned branch, it shall then be deemed that the branch has not complied with these directions, which may attract penal action on the erring staff.

#### 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.

#### **Identification of Beneficial Owner:**

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his / her identity shall be undertaken keeping in view the following :

a. Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdiction notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

b. In cases of trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is determined. In such cases, satisfactory

evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

c. Identification of beneficial owner/s will be in accordance with the Master Directions on KYC issued by the Reserve Bank of India from time to time.

### **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. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. 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 half-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/wealth.

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 06 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 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 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.

### 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.

## **5 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](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.

Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account for meticulous compliance.

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.

c) 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 February 2, 2021 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 February 2, 2021 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 01123092736. 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.

**6 Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):**

(a) All offices shall ensure meticulous compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annexure III of Master Direction of RBI last updated upto 04.05.2023).

(b) In accordance with paragraph 3 of the aforementioned Order, all offices shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, all offices shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) In case of match in the above cases, the transaction details with full particulars of the funds, financial assets or economic resources involved, be immediately reported to the Principal Officer for onward submission of same to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent by the Principal officer to State Nodal Officer, where the account / transaction is held and to the RBI. The Principal Officer shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) All offices may refer to the designated list, as amended from time to time, available on the portal of FIU-India

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, the concerned office shall prevent such individual/entity from conducting financial transactions and immediately inform to Principal Officer for their onward intimating the same to the CNO by email, FAX and by post, without delay.

(g) In case an order to freeze assets under Section 12A is received by the Bank from the CNO, the Bank shall, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall immediately be forwarded by the concerned office to Principal Officer with full details of the asset frozen, as given by the applicant, for their onward submission of the same to the CNO by email, FAX and by post, within two working days.

All offices shall verify every day, the ‘UNSCR 1718 Sanctions List of Designated Individuals and Entities’, as available at <https://www.mea.gov.in/Implementation-ofUNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the ‘Implementation of Security Council Resolution on Democratic People’s Republic of Korea Order, 2017’, as amended from time to time by the Central Government.



In addition to the above, all offices shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

**7. 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.

**8. 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.

**9. 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.

#### **10. 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.

#### **11. 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).

#### **12. Principal Officer**

a) In terms with RBI guidelines, the Bank has a Senior Level Personnel at management level, 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 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.

### **13. 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.

### **14. 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
- 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

### **15. 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.

## **16. 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/>

## **17. 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.

### **b. 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.

#### **18. 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. However, transactions pertaining to funds transfer within same entity should not be reported under NTR (As per guidelines issued vide letter no. 27-3/SAG/2019/FIU-IND dated 08<sup>th</sup> February, 2021)

#### **19. 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. Bank shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff

## **20. Central KYC Records Registry :**

(a) 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.

(b) In terms of provision of Rule 9(1A) of the PML Rules, the bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be.

(d) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, banks are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after April 1, 2017, with CKYCR in terms of the provisions of the Rules *ibid*.

(e) Banks shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the LE Template released by CERSAI.

(f) Once KYC Identifier is generated by CKYCR, bank shall ensure that the same is communicated to the individual/LE by SMS, as the case may be.

(g) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, REs shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per (d) and (e) respectively at the time of periodic updation as specified in Section 38 of Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

(h) Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(i) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to bank, with an explicit consent to download records from CKYCR, then bank shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless – (i) there is a change in the information of the customer as existing in the records of CKYCR; (ii) the current address of the customer is required to be verified; (iii) the bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client. (iv) the validity period of documents downloaded from CKYCR has lapsed.

**21. The present policy will be valid from the date of its approval by the Board of Directors and shall be applicable to both new and existing customers of the bank. The Board may review the policy as and when required or In case there are any regulatory changes requiring modification to the Policy, the Policy shall be reviewed.**

## LIST OF OFFICIALLY VALID KYC DOCUMENTS

**Resident Individuals**

<b>ACCEPTABLE KYC DOCUMENTS</b>	
<b>Valid List of Documents for Proof of Identity &amp; Address</b>	
I. Voter ID Card II. Passport III. Driving License IV. NREGA Job Card & Others V. Letter issued by National Population Register containing details of name, address VI. Job Card issued by NREGA duly signed by an officer of State Government VII. Letter issued by the UIDAI containing details of name, address and Aadhaar number. VIII. Where the OVD furnished by the customer does not have updated address, For the limited purpose of proof of address, the following additional documents are deemed to be OVDs where simplified measures are applied:	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) Latest Property or Municipal/Village panchayat 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, leave and licence agreements with such employers allotting official accommodation; and f) Documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India. Branches shall obtain only the documents as mentioned above and not to accept any other document for KYC purpose.
<p>Branches to ensure to obtain OVD with current address within a period of three months of submitting the documents specified at “VIII” above.</p>	
<b>Mandatory Documents</b>	
<ul style="list-style-type: none"> <li>• <b>Permanent Account Number (PAN) or Form 60</b> (as applicable ) is mandatory</li> </ul>	

**Non Individuals**

Certified copies of following documents or the equivalent e-documents thereof to be obtained duly verified:

<b>ACCEPTABLE KYC DOCUMENTS</b>	
<b>Entity Type</b>	<b>Documents</b>
<b>TRUST</b>	Entity proof and Address proof Documents of the Entity. <ul style="list-style-type: none"> <li>• Trust Deed signed by at least 2 managing / authorized trustees</li> <li>• Certificate of registration with Registrar of Trusts or Deputy / Assistant Charity Commissioner / PF Commissioner (in case of PF Trust)</li> <li>• PAN card in the name of the Trust</li> <li>• Certified copy of the Resolution to open/maintain the Bank account signed by the chairperson/secretary/ 2 authorised signatories or by the authorised trustees as mentioned in trust deed.</li> </ul>

	<ul style="list-style-type: none"> <li>• Names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust</li> <li>• The address of the registered office of the trust</li> <li>• List of trustees and documents as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.</li> <li>• Beneficial owner Declaration.</li> <li>• KYC documents of all signatories</li> </ul>
<p style="text-align: center;"><b>STATUTORY CORPORATIONS</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Resolution for account opening: A request letter with the entity seal / letter head of the entity shall suffice.</li> <li>• Entity proof like Govt. Notification, Letter from the ministry acknowledging the constitution of the entity, etc. or any other document to establish the legal existence of entity</li> <li>• Document showing name of the person authorised to act on behalf of entity.</li> <li>• PAN Card to be taken if applicable for the entity.</li> <li>• Beneficial owner Declaration.</li> <li>• KYC documents of all signatories</li> </ul>
<p style="text-align: center;"><b>SOLE PROPRIETOR</b></p>	<ol style="list-style-type: none"> <li>1. Apart from customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice : <ul style="list-style-type: none"> <li>• Registration certificate including Udyam Registration Certificate (URC) issued by the Government.</li> <li>• Certificate/licence issued by the Municipal authorities under Shop &amp; Establishment Act,</li> <li>• Sales and Income tax returns</li> <li>• CST/VAT/GST certificate</li> <li>• Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities</li> <li>• Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.</li> <li>• 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.</li> </ul> </li> <li>2. KYC documents of Proprietor.</li> <li>3. PAN Card of Proprietor.</li> </ol> <p>Though the default rule is that any two documents mentioned in (1) 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>



<p><b>SOCIETY</b></p>	<p>Entity proof and Address Documents of the Entity.</p> <ul style="list-style-type: none"> <li>• Certified copy of certificate of registration of the society signed by the Secretary / Chairperson / President / Member's of the Managing Committee.</li> <li>• Certified copy of Rules and By-Laws of the society signed by the Secretary / Chairperson / President / Members of the Managing Committee (If available).</li> <li>• PAN card in the name of the Society.</li> <li>• Certified copy of the resolution to open the account signed by the chairperson/secretary/ president/ authorised signatories.</li> <li>• Society's memorandum of association and rules and regulations. (If Available)</li> <li>• Beneficial owner Declaration.</li> <li>• KYC documents of all signatories</li> </ul>
<p><b>PRIVATE LIMITED COMPANY</b></p>	<p>Entity proof and Address proof of the Entity</p> <ul style="list-style-type: none"> <li>• Memorandum of Association ( MOA )</li> <li>• Articles of Association (AOA )</li> <li>• Certificate of Incorporation</li> <li>• Board Resolution (BR) -duly signed to open account</li> <li>• PAN Card in the name of the company</li> <li>• Any documents as mentioned above (except BR) containing address will be acceptable as address proof.</li> <li>• The names of the relevant persons holding senior management position</li> <li>• The registered office and the principal place of its business, if it is different.</li> <li>• Beneficial owner Declaration.</li> <li>• KYC documents of all signatories</li> </ul>
<p><b>PUBLIC LIMITED COMPANY</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Memorandum of Association ( MOA )</li> <li>• Articles of Association (AOA )</li> <li>• Certificate of Incorporation</li> <li>• Board Resolution (BR) - duly signed</li> <li>• PAN Card in the name of the company</li> <li>• Certificate of Commencement of Business</li> <li>• Any documents as mentioned above (except BR) containing address will be acceptable as address proof.</li> <li>• The names of the relevant persons holding senior management position</li> <li>• The registered office and the principal place of its business, if it is different.</li> <li>• Beneficial owner Declaration.</li> <li>• KYC documents of all signatories</li> </ul>
<p><b>PARTNERSHIP FIRM</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Partnership Registration Certificate.</li> <li>• Latest partnership deed copy.</li> <li>• PAN Card copy of Firm.</li> <li>• The names of all the partners</li> <li>• Address of the registered office and the principal place of its business, if it is different.</li> <li>• Beneficial Owner Declaration</li> <li>• KYC Documents of all signatories and Partners.</li> </ul>

<p align="center"><b>LIMITED LIABILITY PARTNERSHIP</b></p>	<p>Entity proof and Address proof of the Entity</p> <ul style="list-style-type: none"> <li>• Certified copy of incorporation documents filed with Registrar of Companies. OR</li> <li>• Certificate issued by the Registrar of Companies.</li> <li>• 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.</li> <li>• The names of all the partners</li> <li>• Address of the registered office and the principal place of its business, if it is different.</li> <li>• PAN Number of the Firm</li> <li>• An officially valid KYC document in respect of the person holding an attorney to transact on its behalf, so also of all the partners.</li> <li>• Beneficial Owner Declaration.</li> </ul>
<p align="center"><b>HUF</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• HUF Declaration duly signed by all adult Co-parceners and naming the Karta, who would be authorised to operate the account.</li> <li>• KYC document of Karta and all adult co-parceners</li> <li>• HUF Deed Copy.</li> <li>• PAN in the name of HUF.</li> </ul>
<p align="center"><b>GOVERNMENT DEPARTMENTS/ Undertakings, Statutory Corporations and Bodies, Quasi / Self Regulators/ Juridical person</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Resolution for account opening: A request letter with the entity seal/ letter head of the entity shall suffice.</li> <li>• Entity proof like Govt. Notification, Letter from the ministry acknowledging the constitution of the entity, etc. or any other document to establish the legal existence of entity</li> <li>• Document showing name of the person authorised to act on behalf of entity.</li> <li>• PAN Card to be taken if applicable for the entity.</li> </ul>
<p align="center"><b>ASSOCIATION</b></p>	<p>Entity proof and Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Certified copy of certificate of registration of the society/Association signed by the Secretary / Chairperson / President / Members of the Managing Committee.</li> <li>• Certified copy of Rules or By-Laws of the Society/Association signed by the Secretary / Chairperson / President / Members of the Managing Committee.</li> <li>• PAN card in the name of the Society/Association.</li> <li>• Certified copy of the resolution to open the account signed by the chairperson/secretary/ president/ authorised signatories.</li> <li>• Beneficial Owner Declaration</li> <li>• KYC Documents of all signatories and Partners.</li> </ul>
<p align="center"><b>Co-operative Banks (CASA accounts &amp; FD's)</b></p>	<p>Entity proof and Address proof of the Entity</p> <ul style="list-style-type: none"> <li>• RBI licence and Registration certificate from State Registrar for Co-operative Societies.</li> <li>• Board Resolution not older than Six months stating authority of account opening and mode of operation duly signed by two members from Managing Committee /Governing Committee/ Board of Directors.</li> <li>• List of authorized signatories with specimen signatures.</li> <li>• PAN Card.</li> <li>• Beneficial Owner Declaration.</li> <li>• KYC Documents of all signatories</li> </ul>

<b>Unincorporated Associations/Body of Individuals</b>	<p>Address proof of the Entity.</p> <ul style="list-style-type: none"> <li>• Any such document to collectively establish the existence of such association/ body of individuals.</li> <li>• List of name and address of the members of the managing committee/ governing body on the letterhead of entity.</li> <li>• Certified copy of the resolution mentioning that the association is unregistered Association of persons and desires to open the bank account in the name of entity with mode of operation and authorised signatories.</li> <li>• Power of attorney granted to transact on its behalf</li> <li>• PAN Card copy of entity.</li> <li>• Beneficial Owner Declaration.</li> <li>• KYC Documents of all signatories</li> </ul>
--	--

**Note: If any of the above Non-individual entity or organisation is constituted for religious or charitable purpose referred to in clause (15) of Section 2 of Income-tax Act, 1961 (43 of 1961) that is registered as trust or a society under Societies Registration Act, 1860 or any similar legislation or company registered under Section 8 of Companies Act, 2013 (18 of 2013) then the said entity or organisation should be classified as Non-profit organisation (NPO).**

**Branches to ensure that in case of customers who are non-profit organisations (NPOs), the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, branches shall request the said customer in writing to get it registered immediately on the DARPAN Portal or may register the details of customers on DARPAN portal. Branches shall also maintain such registration records for a period of five years after the business relationship between the customer and the bank has ended or the account has been closed, whichever is later.**

[As per Sec 2(15) of Income Tax Act 1961 "charitable purpose" includes relief of the poor, education, yoga, medical relief, preservation of environment (including watersheds, forests and wildlife) and preservation of monuments or places or objects of artistic or historic interest, and the advancement of any other object of general public utility:

**Provided** that the advancement of any other object of general public utility shall not be a charitable purpose, if it involves the carrying on of any activity in the nature of trade, commerce or business, or any activity of rendering any service in relation to any trade, commerce or business, for a cess or fee or any other consideration, irrespective of the nature of use or application, or retention, of the income from such activity, unless—

(i) such activity is undertaken in the course of actual carrying out of such advancement of any other object of general public utility; and

(ii) the aggregate receipts from such activity or activities during the previous year, do not exceed twenty per cent of the total receipts, of the trust or institution undertaking such activity or activities, of that previous year;

## **List of Other Valid Entity Documents**

- Any certificate issued for registration/operations/Trade License/business by Local/State/ Central Government/Government Agency/SEBI/IRDA/ICAI/ICSI/ICWAI/Office of Registrar in the name of entity/firm.
- Labour License/Certificate
- Professional Tax Registration Certificate
- Trade Mark Registration Certificate
- Liquor License/Registration Certificate
- Drug License
- Registration Certificate issued by Excise & Customs Department.
- Registration Certificate issued under Weight & Measurement Act
- Police Department License/Certificate
- Regional Transport Office Permit/Registration Certificate
- Consent to Operate issued by State/Central Pollution Control Board
- GST Registration certificate /Sales Tax Registration Certificate/TIN Certificate/VAT Certificate/Service Tax certificate/TAN certificate/Allotment letter for new firms not older than six months.
- Valid Shops & Establishment Certificate/Trade License. Validity can be extended up to the grace period for renewal as mentioned in such certificate.
- Certificate Issued by SEZ, STP, EHTP, DTA and EPZ in the name of the entity mentioning the address allotted.
- Gram Panchayat Certificate (should be on letterhead and not more than 3 month old)  
Branch Manager/ Officer to visit communication address and certify the existence of business activity.
- Trade License in the name of entity.
- Small Scale Industries (SSI) Certificate
- Factory Registration Certificate in the name of entity.
- SEBI Registration Certificate in the name of the entity.
- The Shops and Establishment Certificate issued by the Municipal Corporations

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

<b><u>Low Risk</u></b>	<b><u>Medium Risk</u></b>	<b><u>High Risk</u></b>
1. Cooperative Bank	1. Gas Station	1. Customers with dubious reputation as per public information available or commercially available watch lists
2. Ex-staff, Govt./ Semi Govt. Employees	2. Car / Boat / Plane Dealership	2. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
3. Illiterate	3. Electronics (wholesale)	3. 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.
4. Individual	4. Travel agency	4. 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;
5. Local Authority	5. Used car sales	5. Private Limited Company
6. Other Banks	6. Telemarketers	6. Unregistered body
7. Pensioner	7. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center	7. Pawnshops
8. Public Ltd.	8. Dot-com company or internet business	8. Non face-to-face Customers
9. Public Sector	9. Proprietorship	9. High net worth individuals
10. Public Sector Bank	10. Auctioneers	10. Firms with 'sleeping partners'
11. Staff	11. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.	11. Companies having close family shareholding or beneficial ownership
12. Regional Rural Banks	12. Sole Practitioners or Law Firms (small, little known)	12. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
13. Govt./SemiGovt. Local Body	13. Notaries (small, little known)	13. 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
14. Senior Citizens	14. Secretarial Firms (small, little known)	14. Investment Management / Money Management Company/Personal Investment Company
15. Self Help Groups	15. Accountants (small, little known firms)	15. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.
	16. Venture capital companies	16. Trusts, charities, NGOs/NPOs
	17. Blind	21. Money Service Business: including seller of: Money Orders / Travelers“ Cheques / Money Transmission /
	18. Purdanashin	
	19. Registered Body	
	20. Corporate Body	
	21. Joint Sector	
	22. Partnership	
	23. HUF	
	24. Minor	

		<p>Cheque Cashing / Currency Dealing or Exchange</p> <p>22. Gambling/gaming including “Junket Operators” arranging gambling tours &amp; Casinos</p> <p>23. 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> <p>23. Customers engaged in industries that might relate to nuclear proliferation activities or explosives</p> <p>24. Customers that may appear to be Multi level marketing companies etc.</p> <p>25. Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence)</p> <p>26. Associations/Clubs</p> <p>27. Bullion dealers and Jewellers (subject to enhanced due diligence)</p> <p>28. Other Cash Intensive business</p> <p>29. Customers dealing in Import / Export</p>
--	--	---

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