KYC/AML/CFT POLICY
(DOMESTIC BRANCHES)
2022-23

SP&D Wing
HEAD OFFICE
112, J C ROAD
BENGALURU -560002

INDEX

POLICY GUIDELINES ON KYC/AML/CFT-2022-23 (DOMESTIC BRANCHES)

1. OBJECTIVE

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

The objective of KYC/AML/CFT guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Bank to know/ understand the customers and their financial dealings better and manage the risks prudently. The Board approved policy on KYC/AML/CFT is subject to annual review. If any changes in the policy are required before the annual review on account of changes in the regulations or statutes, the Operational Risk Management Committee of the bank is authorized to make such changes and place the same in the next Board meeting for adoption.

2. DEFINITIONS

2.1 Customer:

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

2.2 Designated Director:

"Designated Director" means a person designated by the bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes the Managing Director or a whole-time Director duly authorized by the Board of Directors.

2.3 Principal Officer:

"Principal Officer" means an officer nominated by the bank, responsible for furnishing information under PMLA Rules.

The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

2.4 Person:

In terms of PML Act a person includes:

i. An individual,
ii. A Hindu Undivided Family,
iii. A company,

iv. A firm,
v. An association of persons or a body of individuals, whether incorporated or not,
vi. Every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. Any agency, office or branch owned or controlled by any of the above persons (i to vi).

2.5 Transaction:

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

(i) Opening of an account;
(ii) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
(iii) The use of a safety deposit box or any other form of safe deposit;
(iv) Entering into any fiduciary relationship;
(v) Any payment made or received in whole or in part of any contractual or other legal obligation; or
(vi) Establishing or creating a legal person or legal arrangement.

2.6 Suspicious transaction:

"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to not have economic rationale or bona-fide purpose; or
(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

2.7 Know Your Client (KYC) Identifier

Know Your Client (KYC) Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.

2.8 Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

i. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

(b) Where the customer is a **partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

(c) Where the customer is an **unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d) Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(e) Where the customer is a Self Help Groups (SHGs) or Joint Liability Group (JLGs), the Office Bearers of SHG/JLG may deemed to be the Senior Managing Officials. Hence, they shall be treated as Beneficial Owners of SHG/JLG.

2.9 Aadhaar Number:

"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

2.10 Certified Copy:

Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the bank.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

• Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
• Branches of overseas banks with whom Indian banks have relationships,
• Notary Public abroad,

- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

2.11 Digital KYC

"Digital KYC" means the capturing the live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the bank.

2.12 Video based Customer Identification Process (V-CIP)

An alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the Bank by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face Customer Identification Process for the purpose of this Policy.

2.13 Equivalent e-document:

Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

"Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

2.14 Officially Valid Document:

The Officially Valid Documents are as under:

(1) Passport.
(2) Driving License.
(3) Proof of possession of Aadhaar number*.
(4) Voter Identity Card issued by Election Commission of India.
(5) Job card issued by NREGA duly signed by an officer of the State Government.
(6) Letter issued by the National Population Register containing details of name and address.

*Where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique

Identification Authority of India (UIDAI) and Proof of possession of Aadhaar shall include the following:

(a) Aadhaar letter issued by UIDAI which carry name, address, gender, photo and date of birth details of the Aadhaar number holder
(b) Downloaded Aadhaar (e-Aadhaar) which carries name, address, gender, photo and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by UIDAI
(c) Aadhaar Secure QR code generated and digitally signed by UIDAI containing carries name, address, gender, photo and date of birth details of the Aadhaar number holder.
(d) Aadhaar paperless offline e-KYC which is an XML document generated by UIDAI and digitally signed by UIDAI containing name, address, gender, photo and date of birth details of the Aadhaar number holder.

In case, Officially Valid Documents (OVDs) furnished by the customer does not contain updated address, the following documents or the equivalent e-documents there of shall be deemed to the OVDs for the limited purpose of proof of address:-

(i) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
(ii) Property or Municipal tax receipt;
(iii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Department or Public Sector Undertakings, if they contain the address;
(iv) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

(The ***Customer*** shall submit updated Officially Valid Document with current address within a period of three months of submitting the above document).

Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

3. KEY ELEMENTS OF KYC POLICY:

The KYC Policy includes the following four key elements:

a) Customer Acceptance Policy (CAP);
b) Customer Identification Procedures (CIP);
c) Monitoring of Transactions; and
d) Risk Management.

3.1 CUSTOMER ACCEPTANCE POLICY (CAP)

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

(i) No account is opened or maintained in anonymous or fictitious / benami name.

(ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Bank in categorizing the customers into low, medium and high risk ones, as detailed in para 3.1.1;

(iii) While opening an account and during the periodic updation, documents and other information to be collected from different categories of customers are detailed in Annexure-I of this Policy.

(iv) Bank will not open an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/ or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. Bank may also consider closing an existing account under similar circumstances.

(v) Optional / Additional information is obtained with the explicit consent of the customer after the account is opened.

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

(vii) Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice of banking.

(viii) Bank shall have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

(ix) Bank shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level. Thus, if an existing KYC compliant customer desires to open another account with our bank, there shall be no need for a fresh CDD exercise.

(x) CDD procedure is followed for all the joint account holders, while opening joint account.

(xi) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

(xii) Where an equivalent e-document is obtained from the customer, bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

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

3.1.1 Risk Perception in respect of Customer:

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

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

Low Risk Customers (Level 1 customers):
Individuals (other than High Networth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as Low Risk, such as:

- Salaried employees.
- People belonging to lower economic strata of the society.
- Government Departments.
- Government owned companies.
- Regulatory and Statutory bodies, etc.

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

Medium Risk Customers (Level 2 customers):
Customers who are likely to pose a higher than average risk to the Bank should be categorised as medium or high risk.

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

An indicative list of **Medium Risk Customers** is as under**:**

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

High Risk Customers (Level 3 customers):
For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank shall subject such accounts to **enhanced monitoring on an ongoing basis**. An indicative list of High Risk customers is as under:

- Trusts, charities, NGOs and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership.
- Firms with 'sleeping partners'.

- Accounts under Foreign Contribution Regulation Act.
- Politically Exposed Persons (PEPs).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers.
- High Net worth Individuals*
- ***Non-Resident customers (Based on the risk profile of 'country where the customer is domiciled)***
- Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewelers.

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

Customers with any of the following:

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

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

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

Customer Risk Categorisation

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

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

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

Risk Parameters

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

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

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

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

Risk rating of Customers:

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

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

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

Account Types	***High***	***Medium***	***Low***
Average Balance in all deposit accounts (SB+ CA+ TD)	Rs.100 lakh & above	Rs. 25 lakh & above but less than Rs.100 lakh	Less than Rs.25 lakh

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

C. Risk Categorization of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:
   - Unusual transaction/behavior (given as Annexure III – Monitoring of Customer Risk Categorisation (CRC).

- Submitted Suspicious Transaction Reports (STR) for Customer.
- Submitted Cash Transaction Report (CTR).
- Frequent Cheque returns.

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

Risk categorization of Customers undertaken by the Bank:

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

i. Customer type.
ii. Customer profession.
iii. Type of business.
iv. Product code.
v. Account status
vi. Account vintage.
vii. Average balance in deposits in SB/Current/Term Deposit accounts.

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

The process of Risk categorization of NRIs shall be based on the risk profile of the 'country where the customer is domiciled'. The risk assigned to all product codes of NRI shall be changed automatically based on the risk profile of the country without change in other parameters of risk categorization. The final risk categorization shall be done taking into consideration the rating in all the seven parameters.

Export Credit Guarantee Corporation of India Ltd (ECGC) is updating the country risk classification on regular basis.

The details of classification is as under:

ECGC CLASSIFICATION	RISK CATEGORY	FINAL RISK ALLOTMENT
A1	Insignificant	**LOW**
A2	Low Risk	
B1	Moderately Low Risk	
B2	Moderate Risk	**MEDIUM**
C1	Moderately High Risk	**HIGH**
C2	High Risk	
D	Very High Risk	

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

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

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

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

When an existing customer opens a new SB/CA account, the vintage parameter need not be taken into account for risk categorization of such accounts and the account may be classified basing on the risk category allotted to the customer on the other 6 parameters.

Once new account completes six months then the account should be categorized as medium subject to complying with other parameters. And the account thereafter should go to low risk after twelve months subject to complying with other parameters.

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

Roles and responsibilities of Branches:

Branches shall review Customer risk categorization based on the risk categorization generated by the system, every six months i.e., **30th Jun and 31st December every year.**

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

Branch shall review Customer risk categorization based on the risk

Roles and responsibilities of Circle Offices:

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

Shall ensure compliance of Risk Categorization at branches every six months by obtaining confirmation from ROs and branches under direct control of CO.

Shall submit periodical reports on implementation/review of risk categorisation to KYC Cell, Central Processing Wing, H.O.

Shall attend/follow-up audit observations/remarks.

Roles and responsibilities of Regional Offices:

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

Shall ensure compliance of Risk Categorization at branches every six months.

Shall submit periodical reports on implementation/review of risk categorisation to Circle Office.

Shall attend/follow-up audit observations/remarks.

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

Oversee implementation/monitoring and review of risk categorization of customers by putting in place suitable reporting/monitoring mechanism.

Ensure proper maintenance of MIS for customer risk categorization and migration data.

Shall review fixing of parameters available through the system annually.

SP&D Wing along with Technology Operations Wing shall identify the parameters available in the system for risk categorization through the system as per the model suggested in the policy.

KYC Cell & Re-KYC Cell, Central Processing Wing, H.O:

Shall review and provide necessary recommendations/directions to strengthen adherence of KYC guidelines.

Shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

Monitoring/Review of Customer Risk Categorisation (CRC):

The review of risk categorization of customer's accounts and updation thereof (Wherever necessary) shall be carried out on daily basis with a periodicity of 6 months.

During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.

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

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

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

Monitoring of Customer Risk Categorisation (CRC) – given as Annexure III to this Note.

3.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification means undertaking the process of CDD (Customer Due Diligence i.e. Identifying and verifying the customer and the beneficial owner).

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

Bank shall have a policy approved by the Board which clearly spells out the Customer Identification Procedure to be carried out at different stages, i.e.,

(i) While establishing a banking relationship;
(ii) While carrying out a financial transaction;
(iii) Carrying out any international money transfer operations for a person who is not an account holder of the bank.
(iv) When the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;
(v) When bank sells third party products as agent;
(vi) While selling Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000/-.
(vii) When carrying out transactions for a non-account based customer, that is a walk-in-customer, where the amount is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected;
(viii) When the Bank has reason to believe that a customer (account based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.
(ix) Bank shall ensure that introduction is not to be sought while opening accounts.

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

Customer Due Diligence requirements (CDD) while opening accounts

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

Branches shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for

'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

KYC data of individual accounts is to be uploaded to Central KYC Registry (CKYCR) within T+5 days from the date of establishing account based relationship.

Branches shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017 with CKYCR. In order to ensure that all existing KYC records of individual customers are incrementally uploaded on to CKYCR, Branches shall upload the KYC data pertaining to accounts of individuals opened prior to January 01, 2017, at the time of periodic updation or earlier when the updated KYC information is obtained/received from the customer in certain cases.

As the CKYCR is now fully operational for individual customers, it has been decided to extend the CKYCR to Legal Entities (LEs). Accordingly, Branches shall upload the KYC data pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of Rule 9 (1A) of the PML Rules. The KYC records shall be uploaded as per the LE Template released by CERSAI.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Branches shall upload/update the KYC data pertaining to accounts of Legal Entities opened prior to April 1, 2021, at the time of periodic updation or earlier, when the updated KYC information is obtained/received from the customer.

Once KYC Identifier is generated by CKYCR, it is to be ensured that the same is communicated to the individual/legal entity as the case may be

It is to be ensured that during periodic updation, the customers' KYC details are migrated to current Customer Due Diligence (CDD) standards.

Where a customer, for the purpose of establishing an account based relationship, submits a KYC Identifier, with an explicit consent to download records from CKYCR, then such branch shall retrieve the KYC records online from 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 –

a) There is a change in the information of the customer as existing in the records of CKYCR;

b) The current address of the customer is required to be verified;

c) The branch 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.

3.2.2 Accounts of individuals:

For undertaking Customer Due Diligence (CDD), Bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with

the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

(A) The Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank; or

(B) The proof of possession of Aadhaar number where offline verification can be carried out; or

(C) The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

(D) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(E) Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank.

Provided that where the customer has submitted,

i) Aadhaar number under clause (A) above to a bank, such bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.

ii) Proof of possession of Aadhaar under clause (B) above where offline verification can be carried out, the bank shall carry out offline verification.

iii) An equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

iv) Any OVD or proof of possession of Aadhaar number under clause (C) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC.

Provided that for a period not beyond such date as may be notified by the Government for a class of Regulated entities, instead of carrying out digital KYC, the Regulated entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

3.2.3 e-KYC services of UIDAI

In case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the

Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer.

CDD done in this manner shall invariably be carried by an authorized official of the bank and such exception handling shall also be a part of the concurrent audit.

Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits proof of possession of Aadhaar number containing his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 ***and the regulations made thereunder***.

3.2.4 Introduction of accounts:

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

3.2.5 Accounts of married women:

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

Accordingly, Branches shall accept a copy of marriage certificate issued by the State Government or Gazette notification indicating change in name, together with a certified copy of the 'Officially Valid Document' in the existing name of the person while establishing an account based relationship or while undergoing periodic updation exercise.

3.2.6 Small Accounts:

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

The "Canara Small Savings Bank Deposit" account can be opened by production of a self-attested photograph and affixation of signature or thumb impression, as the case may be, on the Account Opening form. The designated bank official, while opening the small account, should certify under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence.

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

(i) Accounts where aggregate of all credits in a financial year does not exceed Rs.1.00 lakh;
(ii) The aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000/- and
(iii) Where the balance at any point of time does not exceed Rs.50,000/-

The above limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

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

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

A Canara Small Savings Bank Deposit Account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the Bank of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months. ***Notwithstanding anything contained in the clauses, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government***.

The small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of Officially Valid Documents.

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

Where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the office in-charge of the jail.

3.2.7 Basic Savings Bank Deposit Accounts

As per RBI guidelines, the Basic Savings Bank Deposit Account should be considered a normal banking service available to all.

The Basic Savings Bank deposit Account is subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time. If such account is opened on the basis of simplified KYC norms, the account would additionally be treated as a "Small Account" and would be subject to conditions stipulated for small accounts.

- In case the address mentioned as per 'proof of address' undergoes a change, the document mentioned in point no 2.14 is to be obtained for limited period and the customer has to submit updated Officially Valid Document with current address within a period of three months of submitting the above document).
- Branches are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the Bank to another branch. KYC once done by one branch of the Bank shall be valid for transfer of the account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customer shall be allowed to transfer his account from one branch to another branch without restrictions.
- If an existing KYC compliant customer of the Bank desires to open another account in the Bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

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

(a) Records of the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
(b) The branch takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
(c) The branch is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;
(d) The third party is not based in a country or jurisdiction assessed as high risk; and
(e) The branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

3.2.9 Account opened using OTP based e-KYC, in non-face-to-face mode

The bank may open accounts using OTP based e-KYC in non-face-to-face mode subject to the following conditions:

(i) There must be a specific consent from the customer for authentication through OTP.
(ii) The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
(iii) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
(iv) As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
(v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year ***unless identification as per above para 3.2.2 or as V-CIP is carried out. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.***
(vi) If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts, no further debits shall be allowed.
(vii) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Regulated Entity. Further, while uploading KYC information to CKYCR, the bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Regulated Entities shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
(viii) The bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

3.2.10 Accounts of non-face-to-face customers (Other than Aadhaar OTP based on-boarding):

"Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of Banks'.

Bank shall ensure that the first payment is to be effected through the customer's KYC-complied account with another bank, for enhanced due diligence of non-face-to-face customers.

3.2.11 Video Based Customer Identification Process (V-CIP):

Bank may undertake V-CIP to carry out:

i. Customer Due Diligence (CDD) in case of new customer on-boarding for individual customers, proprietor in case of Proprietorship firm, authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a Proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the Proprietorship firm, as mentioned in Para no. 3.2.13, apart from undertaking CDD of the Proprietor.

ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.

iii. Updation/Periodic updation of KYC for eligible customers.

Bank opting to undertake V-CIP, shall adhere to the following minimum standards:

(A) <u>V-CIP INFRASTRUCTURE</u>:

i) The Bank should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

ii) The Bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber-event under extant regulatory guidelines.

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance

strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(B) V-CIP PROCEDURE:

i) **Each Bank shall formulate a clear work flow and standard operating procedure** *for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Bank specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.*

ii) If **there** *is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.*

iii) *The sequence and/or type of questions, including those indicating the liveness* **of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.**

iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

vi) **The authorized official of the Bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification** *and obtain the identification information using any one of the following:*

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with Para 3.2, using the KYC identifier provided by the customer

d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Bank shall ensure to redact or blackout the Aadhaar number in terms of **Section 16.**

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

Further, *in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Bank shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Bank shall ensure that no incremental risk is added due to this.*

vii) If the address *of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.*

viii) Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

x) The authorised official of the Bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank.

(C) <u>V-CIP RECORDS AND DATA MANAGEMENT</u>

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as per RBI Guidelines, shall also be applicable for V-CIP.

ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

3.2.12 <u>Accounts of Foreign students studying in India:</u>

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

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

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

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

d) The account would be treated as a normal NRO account after verification of address and will be operated in terms of existing guidelines issued in the Manual of instructions on Non-Resident Deposits and Circulars issued from time to time.

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

3.2.13 Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/ Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Bank shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. Branches shall maintain a database of PEP accounts in the Branch. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

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

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

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

3.2.14 Accounts of persons other than individuals:

Bank needs to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Bank shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be

moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

(i) Accounts of Companies

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

(i) Certificate of incorporation
(ii) Memorandum and Articles of Association
(iii) Permanent Account Number of the company
(iv) A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf.
(v) Corporate Identification Number (CIN)
(vi) One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of related *beneficial owner*, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

(ii) Accounts of Partnership firms

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

(i) Registration Certificate
(ii) Partnership Deed
(iii) Permanent Account Number of the partnership firm
(iv) One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of related beneficial owner, managers, officers or employees, as the case may be, holding and an attorney to transact on its behalf.

(iii) Accounts of Trusts

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

(i) Registration Certificate
(ii) Trust Deed
(iii) Permanent Account Number or Form No.60 of the trust
(iv) One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the related beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

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

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

(i) Resolution of the managing body of such association or body of individuals
(ii) Permanent Account Number or Form No.60 of the unincorporated association or a body of individuals

(iii) Power of Attorney granted to the person who will transact on its behalf.
(iv) One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the related beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
(v) Such information as may be required to ***collectively*** establish the legal existence of such association or body of individuals.

Note:

(a) Unregistered trusts/partnership firms shall be included under the term 'Unincorporated Association'.
(b) Term 'body of individuals' includes societies.

(v) Accounts of Proprietary Concerns

For Proprietary concerns, Customer Due Diligence of the individual (proprietor) are to be carried out and any two of the following documents or *the equivalent e-document*s in the name of the proprietary concern should be submitted ***as a proof of business/activity:***

a) Registration Certificate
b) Certificate/license issued by the Municipal authorities under Shop & Establishment Act.
c) Sales and income tax returns.
d) CST/VAT/GST certificate (Provisional/Final),
e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
f) 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.
g) Utility bills such as electricity, water and landline telephone bills.
h) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

(vi) For opening accounts of juridical persons not specifically covered above, such as Societies , Universities and Local bodies like Village Panchayats:

The certified copies of the following documents or the equivalent e-documents thereof are to be submitted:

i) Document showing name of the person authorized to act on behalf of the entity;
ii. (a) Any Officially Valid Document which contains proof of identity/address in respect of person holding an attorney to transacts on its behalf and

(b) PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf.
iii) Such documents as may be required to establish the legal existence of such an entity/juridical person

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

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex V, subject to Income Tax (FATCA/CRS) Rules.

Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex V will be submitted.

(viii) Client accounts opened by professional intermediaries:

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

3.2.15 Identification of Beneficial Ownership

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 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 a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) 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.

3.2.16 Accounts of Non Profit Organsiations

A Non-Profit Organization (NPO) means any entity or organization that is registered as a Trust or a Society under the Societies Registration Act, 1860 or any similar State Legislation or a company registered under Section 8 of the Companies Act 2013. All transactions involving receipts by these NPOs of value more than Rs.10 lac or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 lac; the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

3.2.17 Accounts operated by Power of Attorney Holders/Letter of Authority Holders:

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

3.2.18 Introduction of New Technologies - Credit cards / debit cards / smart cards / gift cards / Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

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

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

3.2.19 Periodic updation of KYC

A. CDD requirements for periodic updation:

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account/last KYC updation, as per the following procedures:

(I) ***INDIVIDUAL CUSTOMER:***

i) 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 by way of a letter.

ii) Change in address:

In case of a change in the address details of the customer, Branches shall obtain a copy of Officially Valid Document (OVD) or deemed OVD or the equivalent e-documents thereof for the purpose of proof of address, declared by the customer at the time of periodic updation.

iii) 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, branches to ensure that KYC documents are based on current Customer Due Diligence (CDD) standards. Wherever required, Branches 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.

(II) <u>CUSTOMERS OTHER THAN INDIVIDUALS:</u>

i) 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 a letter from an official authorized by the LE in this regard, Board resolution etc. Further, Branches 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.

ii) Change in KYC information:

In case of change in KYC information, Branches shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

(III) <u>ADDITIONAL MEASURES:</u>

In addition to the above, Branches shall ensure the following:

- *Branches shall ensure that available KYC documents of the customer are based on latest guidelines on required documents before opening of account. This is applicable even if there is no change in customer information but the documents available with the branch are not as per the current Customer Due Diligence (CDD) standards. Further, in case the validity of the CDD documents has expired at the time of periodic updation of KYC, Branches shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.*
- *Customer's PAN detail, if available with the branch, is verified from the database of the issuing authority at the time of periodic updation of KYC. Branches shall verify the PAN details in designated screen.*
- *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.

- ***In order to ensure customer convenience in cases where individual customers express difficulty in approaching the home branch due to age related or other issues, such customers may approach the Branch Head or Section in charge of a non-home Branch, who shall obtain the necessary KYC documents along with the details as per bank format from the customer, attest the same and immediately send to the home branch for updation in CBS.***
- ***In case of Non-Individual and Corporate customers, collection of KYC details for Re-KYC and updation of the same in CBS is to be done by home Branch only.***

B. Temporary ceasing of operations:

In case of existing customers, Bank shall obtain the Permanent Account Number or Form No.60, by such date as may be notified by the Central Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the bank shall give the client an accessible notice and a reasonable opportunity to be heard. Further, bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a bank gives in writing that he does not want to submit his Permanent Account Number or Form No.60, Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

3.2.20 Miscellaneous

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

Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in-customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking

arrangements, branches maintaining/opening such accounts should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, branches should retain the right to verify the records maintained by the client cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements.

B. Operation of Bank Accounts & Money Mules

Money Mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering. "Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In order to minimize the operations of such mule accounts, Branches should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

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

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

(a) KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.

(b) Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

D. Walk-in Customers

Walk-in Customer" means a person who does not have an account-based relationship with the Bank, but undertakes transactions with the Bank.

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

If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/-, the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND.

Branches shall ensure to capture Walk-in Customer details mandatorily while carrying out Cash transactions for a non-account based Customer. Bank shall also verify the identity of the customers for all international money transfer operations.

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

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

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

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

F. Unique Customer Identification Code

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

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

Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency.

The guidelines on "Prohibition on dealing in Virtual Currencies (VCs)" was set aside by the Hon'ble Supreme Court. Hence, Branches shall ensure to carry out Customer Due Diligence of Customers involved in dealing with Virtual Currencies.

H. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected. Banks shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

3.3 MONITORING OF TRANSACTIONS:

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

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

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

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

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

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

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

(v) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts

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

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

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

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

g) Branches are advised to mandatorily obtain either PAN or equivalent e-document and verify while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time or Form 60 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs. 50,000/- and above. If the customer appears to be structuring the transactions into a serious of transactions below the threshold of Rs. 50,000/-, branches are required to obtain PAN or Form 60 (if PAN is not available) from the customer. Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of obtention of PAN or Form 60, wherever the aggregate amount of transactions is Rs. 50,000/- and above.

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

3.4 RISK MANAGEMENT:

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

Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, operational and legal risk arising from such accounts, Bank shall aggregate and monitor significant balances and activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

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

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

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

Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

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

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

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

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

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

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

4. CORRESPONDENT BANKING AND SHELL BANK:

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

(a) Bank shall gather sufficient information to fully understand the nature of the business of the bank including information on management, major business activities,

level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country.

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

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

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

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

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

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

(h) Bank shall not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group).

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

5. WIRE TRANSFERS:

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

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

(i) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
(ii) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
(iii) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
(iv) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

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

The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, Bank shall ensure that all wire transfers are accompanied by the following information.

Cross-border wire transfers

(i) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information.
(ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

Domestic wire transfers

I. Information accompanying all domestic wire transfers of Rs. 50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
II. If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank shall insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.
III. When a credit or debit card is used to effect money transfer, necessary information as (i) above should be included in the message.
IV. Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

(c) Exemptions

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

(d)Role of Ordering, Intermediary and Beneficiary Banks

(i) Ordering Bank

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

(ii) Intermediary Bank

For both cross-border and domestic wire transfers, Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) as the receiving Intermediary Bank, of all the information received from the Ordering Bank.

(iii) Beneficiary Bank

A Beneficiary Bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. As Beneficiary Bank, the Bank shall also take up the matter with the Ordering Bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

6. MAINTENANCE OF KYC DOCUMENTS AND PRESERVATION PERIOD

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

6.1 Maintenance of records of transactions

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

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

6.2 Preservation of Records

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

(i) Bank shall maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including

the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

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

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

7. COMBATING FINANCING OF TERRORISM (CFT)

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

(a) The ISIL (Da'esh) & Al-Qaida Sanctions List includes names of individuals, groups, undertakings and entities associated with the ISIL (Da'esh) /Al-Qaida. The updated ISIL (Da'esh) /Al-Qaida Sanctions List is available at ***https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl***

(b) The 1988 Sanctions List consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban, which is available at ***https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.***

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

Branches are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed customer does not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account. AML/CFT Centralised Unit, Head Office will also cross check the details of all existing accounts with the updated list, on a regular basis. If the particulars of any of the account/s have resemblance with those appearing in the list, branches have to verify transactions carried out in such accounts and report those accounts to AML/CFT Centralized Unit, HO for onward submission to RBI/Financial Intelligence Unit-INDIA apart from advising Ministry of Home Affairs as required under UAPA notification dated ***February 2, 2021***.

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

(a) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an

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

(b) Bank shall strictly follow the procedure laid down in the UAPA Order dated ***February 2, 2021*** (**Annexure IV to this Policy**) and ensure meticulous compliance to the Order issued by the Government. ***The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs***.

7.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations

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

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

8. REPORTING REQUIREMENTS

(a) Reporting to Financial Intelligence Unit-India

(i) In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations [NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under (erstwhile Section 25 of Companies Act, 1956) Section 8 of the Companies Act, 2013], cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

The Director, FIU-IND,Financial Intelligence Unit-India, 7th Floor, Jeevan Bharti Building, Tower-II, Connaught Place, Sansad Mard, New Delhi-110001.Website - http://fiuindia.gov.in/

(ii) FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. FIU –INDIA in their REPORTING FORMAT GUIDE, informed that for account based transaction, bank shall report in ACCOUNT BASED REPORTING FORMAT (ARF) and wherever transaction without account based relationship with the customer, bank shall report in TRANSACTION BASED REPORTING FORMAT (TRF).

(iii) In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. ***Branches/Offices/Sections*** shall take note of the timeliness of the reporting requirements and submit the reports within the timelines.

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

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

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

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

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

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

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

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

The Bank shall scrupulously adhere to the following:

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

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

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

iv. ***All accounts where the summation of cash transaction exceeds 10 lakhs either by way of credit or debit in a month are to be reported under CTR.*** A summary of cash transaction report for the Bank as a whole shall be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted to FIU-IND. In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under Core Banking Solution at one point for onward transmission to FIU-IND, provided the CTR is generated in the format prescribed by FIU-IND.

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

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

2. Suspicious Transaction Reports (STR)

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

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

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

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

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

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

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

(i) AML/CFT Centralized Unit, ***Central Processing Wing, HO*** shall process the AML alerts generated / reported. AML team at Circle Offices shall also process the AML alerts and escalate suspicious transactions, if any, to AML/CFT Centralized Unit, ***Central Processing Wing*** ,HO for review and submission of STRs to FIU-IND, Delhi.

(ii) The Manager–in-charge of BS&IC Section at Circle would be the Anti-Money Laundering Officer (AMLO). The Executive overseeing BS&IC Section would be the Money laundering Reporting Officer (MLRO).

(iii) Alerts closed by Circle AMLOs shall be reviewed by Circle MLRO and HO AMLOs.

(iv) AML/CFT Centralized Unit, ***Central Processing Wing, HO*** would review the alerts escalated by the Circles as suspicious transactions and submit STRs wherever required to FIU-IND.

(v) HO MLRO shall review the alerts closed by the HO AMLOs.

3. Money Laundering and Terrorist Financing Risk Assessment:

(i) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

(ii) The risk assessment shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. Further, the periodicity of risk assessment exercise shall be annually.

(iii) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

The internal risk assessment should be conducted by AML/CFT Centralized Unit, Head Office in collaboration with Risk Management Wing, Head Office, ***"Annually"***.

4. Non-Profit Organisation (NPO)

The report of all transactions involving receipts by non-profit organizations of value more than Rupees ten lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

5. *Counterfeit Currency Report (CCR):*

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer of the Bank to FIU-IND in the specified format (Counterfeit Currency Report- CCR) within 15th of the succeeding month. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form. ***Monthly consolidated data to be submitted by the concerned BS&IC Sections of Circle Offices, covering details of such reporting of branches/currency chests falling under their jurisdiction.***

6. Cross-border Wire Transfer Report

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

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

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

***(c)* <u>Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)</u>**

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

"IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

Under FATCA and CRS, Bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

a) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login - -> My Account --> Register as Reporting Financial Institution,
b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
f) Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following:
    i. Updated Guidance Note on FATCA and CRS
    ii. A press release on 'Closure of Financial Accounts' under Rule 114H (8).

9. GENERAL GUIDELINES:

9.1 Confidentiality of customer information:

The information collected from the customer for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling etc. Information sought from the customer shall be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer shall be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

9.2 Secrecy Obligations and Sharing of Information:

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

While considering the requests for data/ information from Government and other agencies, Bank shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions. The exceptions to the said rule shall be as under:

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

9.3 Hiring of Employees:

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

9.4 Employee Training:

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

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

9.5 Accounts under Foreign Contribution Regulation Act, 2010 (FCRA):

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

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

Amendment has been issued vide Gazette notification dated September 28, 2020 regarding the Foreign Contribution (Regulation) Amendment Act, 2020, by the Ministry of Home Affairs (MHA), Government of India, notified on September 28, 2020; and is in force w.e.f September 29, 2020.

In terms of the amended Section 17 of the above-mentioned amendment act, every person/ NGO/ association who have been granted FCRA certificate of registration under FCRA 2010 and prior permission to receive foreign contribution shall henceforth receive such contribution only in an account designated as "FCRA Account" in the specified branch (Main Branch) of State Bank of India (SBI) at New Delhi. No person/ NGO/ association shall receive foreign contributions received in accordance with the FCRA 2010 in any account other than the one designated as "FCRA Account" as per section 17(1) of the FCRA Act, 2010 in the specified branch, i.e., New Delhi Main Branch of the SBI, Sansad Marg, New Delhi, post opening of such an account.

In terms of section 46 of the Foreign Contribution (Regulation) Act, 2010, on the advice of MHA, RBI has instructed all the scheduled banks to stop receiving/ crediting with effect from April 01, 2021 any foreign contributions in any account other than the "designated FCRA Account" in the aforesaid branch of the SBI at New Delhi, which

has been opened by the person who has been granted certificate or prior permission under the FCRA, 2010. The period from September 29, 2020 till March 31, 2021 will be treated as transition period to facilitate opening of the designated "FCRA Account".

MHA has also clarified that the person/ NGO/ association would be free to retain their present account as "other FCRA Account" in any branch of a scheduled bank of their choice which they can link with the "designated FCRA Account" opened in the SBI, New Delhi Main Branch as specified by the Central Government. All foreign contributions shall be received only in the "designated FCRA Account" with the SBI from the date of opening of such account or ***July 01, 2021***, whichever is earlier.

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

9.6 Technology requirements:

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

9.7 Designated Director on the Board of the Bank:

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

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

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

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

9.8 Principal Officer:

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

Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

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

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

The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.
The Principal Officer under PMLA Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

9.9 Need for photographs and address confirmation:

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

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

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

Photograph should be obtained in case of NRI accounts also.

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

9.10 Sale of third party products:

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

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

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

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

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

****

ANNEXURE- I

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

Features		Documents
Accounts of individuals		
	Proof of Identity and Address	For undertaking Customer Due Diligence (CDD), Bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity: **(A)** The Aadhaar number where, (i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or (ii) he decides to submit his Aadhaar number voluntarily to a bank; or **(B)** The proof of possession of Aadhaar number where offline verification can be carried out; or **(C)** The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and **(D)** The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and **(E)** Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank. Provided that where the customer has submitted, i) Aadhaar number under clause (A) above to a bank, such bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

		Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank. ii) Proof of possession of Aadhaar under clause (B) above where offline verification can be carried out, the bank shall carry out offline verification. iii) An equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo. iv) Any OVD or proof of possession of Aadhaar number under clause (C) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC. Provided that for a period not beyond such date as may be notified by the Government for a class of Regulated entities, instead of carrying out digital KYC, the Regulated entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted. • Officially Valid Documents (OVD) are as under: I. Passport II. Driving License III. Proof of possession of Aadhaar number IV. Voter Identity Card issued by Election Commission of India V. Job Card issued by NREGA duly signed by an officer of the State Government VI. Letter issued by the National Population Register containing details of name and address.
Accounts of companies		
		Where the client is a company, certified copies of following documents or the equivalent e-documents are to be submitted: (i) Certificate of incorporation (ii) Memorandum and Articles of Association (iii) Permanent Account Number of the company (iv) A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its

		behalf. (v) Corporate Identification Number (CIN) ***(vi)*** One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of related beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
Accounts of partnership firms		
		Where the client is a partnership firm, certified copies of following documents or the equivalent e-documents are to be submitted: (i) Registration Certificate (ii) Partnership Deed (iii) Permanent Account Number of the partnership firm ***(iv)*** One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of related beneficial owner, managers, officers or employees, as the case may be, holding and an attorney to transact on its behalf.
Accounts of Trusts		
		Where the client is a Trust, certified copies of following documents or the equivalent e-documents are to be submitted: (i) Registration Certificate (ii) Trust Deed (iii) Permanent Account Number or Form No.60 of the trust ***(iv)*** One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the related beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
Accounts of Unincorporated Association or body of individuals		
		Where the client is an unincorporated association or a body of individuals, certified copies of following documents or ***the equivalent e-documents*** are to be submitted: (i) Resolution of the managing body of such association or body of individuals

		(ii) Permanent Account Number or Form No.60 of the unincorporated association or a body of individuals (iii) Power of Attorney granted to the person who will transact on its behalf. (iv) One copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 of the related beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. (v) Such information as may be required to establish the legal existence of such association or body of individuals. **Note:** (a) Unregistered trusts/partnership firms shall be included under the term 'Unincorporated Association'. **(b)** Term 'body of individuals' includes societies.
Accounts of juridical persons not specifically covered above, such as Societies , Universities and Local bodies like Village Panchayats,		
		The certified copies of the following documents or the equivalent e-documents thereof are to be submitted: i) Document showing name of the person authorized to act on behalf of the entity; ii. (a) Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf and *(b)* PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf. iii*) Such documents as may be required to establish the legal existence of such an entity/juridical person.*
Accounts of Proprietorship Concerns		
	Proof of name, address and activity of the concern	For Proprietary concerns, Customer Due Diligence of the individual (proprietor) are to be carried out and any two of the following documents or the equivalent e-documents in the name of the proprietary concern should be submitted ***as a proof of business/activity***: ~~a)~~ Registration Certificate b) Certificate/licence issued by the Municipal authorities under Shop & Establishment Act. c) Sales and income tax returns. d) CST/VAT/GST certificate (Provisional/Final),

		e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities. f) 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. g) Utility bills such as electricity, water and landline telephone bills. h) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.
Accounts of Limited Liability Partnerships		
	Proof of name, address and activity of the concern	(i) Certified copy of incorporation documents filed with Registrar of Companies. (ii) Certificate issued by the Registrar of Companies. (iii) Copy of LLP Agreement signed by all the partners. In case, there is no LLP agreement, Schedule I of the LLP Act signed by all the partners will prevail. (iv) (a) Any Officially Valid Document which contains proof of identity/address in respects of person holding an attorney to transacts on its behalf and *(b)* PAN or Form 60 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf.
Branches to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.		

ANNEXURE- II

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

APPENDIX – A

Low Risk	Medium Risk	High Risk
1. Cooperative Bank 2. Ex-staff, Govt./ Semi Govt. Employees 3. Illiterate 4. Individual 5. Local Authority 6. Other Banks 7. Pensioner 8. Public Ltd. 9. Public Sector 10. Public Sector Bank 11. Staff 12. Regional Rural Banks 13. Govt./Semi-Govt. Local Body 14. Senior Citizens 15. Self Help Groups	1. Gas Station 2. Car / Boat / Plane Dealership 3. Electronics (wholesale) 4. Travel agency 5. Used car sales 6. Telemarketers 7. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center 8. Dot-com company or internet business 9. Pawnshops 10. Auctioneers 11. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc. 12. Sole Practitioners or Law Firms (small, little known) 13. Notaries (small, little known) 14. Secretarial Firms (small, little known) 15. Accountants (small, little known firms) 16. Venture capital companies 17. Blind 18. Purdanashin 19. Registered Body	1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc. 2. Individuals or entities listed in the schedule to the order under Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities 3. Individuals and entities in watch lists issued by Interpol and other similar international organizations 4. Customers with dubious reputation as per public information available or commercially available watch lists 5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk 6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the Customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc. 7. Customers based in high risk countries/jurisdictions or locations (refer **Appendix C**) 8. Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; 9. **Non-resident Customers (Based on the risk profile of 'country where**

	20. Corporate Body 21. Joint Sector 22. Partnership 23. Private Bank 24. Private Limited Company 25. Unregistered body 26. Proprietorship	**the customer is domiciled)** 10. Embassies / Consulates 11. Off-shore (foreign) corporation/ business 12. Non face-to-face Customers 13. High net worth individuals 14. Firms with 'sleeping partners' 15. Companies having close family shareholding or beneficial ownership 16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale 17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence 18. Investment Management / Money Management Company/Personal Investment Company 19. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc. 20. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies) 21. Money Service Business: including seller of: Money Orders / Travelers' Cheques / Money Transmission / Cheque Cashing / Currency Dealing or Exchange 22. Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques/cash payroll cheques) 23. Gambling/gaming including "Junket Operators" arranging gambling tours 24. Dealers in high value or precious goods

		(e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers) 25. Customers engaged in a business which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries) 26. Customers engaged in industries that might relate to nuclear proliferation activities or explosives 27. Customers that may appear to be Multi level marketing companies etc. 28. Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence) 29. Associations/Clubs 30. Foreign Nationals 31. NGO 32. Overseas Corporate Bodies 33. Bullion dealers and Jewelers (subject to enhanced due diligence) 34. Pooled accounts 35. Other Cash Intensive business 36. Shell Banks – Transactions in corresponding banking 37. Non-Bank Financial Institution 38. Stock brokerage 39. Import / Export 40. Executors/Administrators 41. HUF 42. Minor 43. Accounts under Foreign Contribution Regulation Act
The above categorization of customers under risk perception is only illustrative and not exhaustive.		

APPENDIX – B

High / Medium Risk Products and Services

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

Indicative list of High / Medium Risk Products and Services

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

APPENDIX – C

High / Medium Geographic risk

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

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

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

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

Indicative List of High / Medium Risk Geographies

Countries/Jurisdictions

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

Locations

1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations/cities and affected districts)
2. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
3. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

NOTE:

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

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

ANNEXURE-III

Monitoring of Customer Risk Categorisation (CRC):

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

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

Transactions involving large amounts of cash:

- Exchanging an unusually large amount of small denomination notes for those of higher denomination.
- Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.
- Frequent withdrawal of large amounts by means of cheques, including traveler's cheques.
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
- Large cash withdrawals from a previously dormant/ inactive account, or from an account which has just received an unexpected large credit from abroad.
- Company transactions, both deposits and withdrawals that are denominated by unusually large amounts of cash rather than by way of debits and credits normally associated with the normal commercial operations of the company e.g.

cheques , letters of credit , bills of exchange etc.

- Depositing cash by means of numerous credit slips by a customer, such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense:

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

Activities not consistent with the customer's business:

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

Attempts to avoid reporting/ record- keep requirements:

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

Unusual Activities

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

Customer who provides insufficient or suspicious information

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

frequent large transactions.

<u>Certain suspicious funds transfer activities:</u>

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

Annexure- IV

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

1 Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) reads as under:-

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

a. freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
b. prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
c. prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under: -

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

2 In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:

3 Appointment and communication details of the UAPA Nodal Officers:

3.1 *The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA* ***[Telephone Number: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].***
3.2 *The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.*
3.3 *All the States and UTs shall appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.*
3.4 *The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.*

3.5 *The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies.*

3.6 *The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.*

4 Communication of the list of designated individuals/entities:

4.1 *The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988 Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA.*

4.2 *The Financial Regulators shall forward the list of designated persons as mentioned in Para 4(i) above, without delay to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies.*

4.3 *The Central [designated] Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 4(i) above, to all the UAPA Nodal Officers of States/UTs without delay.*

4.4 *The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay.*

4.5 *The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.*

5 Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc.

5.1 The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by the SEBI and insurance companies requiring them -

i. To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, 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, stocks, Insurance policies etc., with them.

ii. In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

iii. The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in 5.1 (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and to Regulators and FIU-IND, as the case may be, without delay.

iv. In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No.011-23092551 and also convey over telephone No.011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

v. The banks, stock exchanges/depositories, intermediaries regulated by SEBI, and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.

5.2 On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/ entities identified by the banks, stock exchanges/depositories, intermediaries and insurance companies are the ones listed as designated individuals/ entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

5.3 In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The Central [designated] Nodal Officer for the UAPA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual/entity.

6 Regarding financial assets or economic resources of the nature of immovable properties:

***6.1** The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given*

parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction, without delay.

6.2 *In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.*

6.3 *The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.*

6.4 *The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.*

6.5 *In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.*

The order shall be issued without prior notice to the designated individual/entity.

6.6 *Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.*

7 Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs):

i. The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.

ii. *The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not carry out such transaction and without delay inform the CBIC, who in turn follow the similar procedure as laid down in the paragraphs 6.2 to 6.5 above.*

iii. *The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organizations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laid down in the paragraphs 6.2 to 6.5 above. The Registrar should also be advised that no societies/ firms/ non-profit organizations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in turn, follow the procedure laid down in the paragraphs 6.2 to 6.5 above.*

iv. *The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraph 6.2 to 6.5 above.*

v. *The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to sensitize their respective members to the provisions of Section 51A of UAPA, so that if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.*

vi. *The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any of designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.*

vii. *In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.*

viii. *The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms. Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.*

8 Regarding implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001:

8.1 *The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.*

8.2 *To give effect to the requests of foreign countries under the 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 Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.*

8.3 *The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND and to the Nodal Officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.*

9 Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

10 Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.

10.1 *The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:-*

a. necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the ntention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

b. necessary for extraordinary expenses, provided that such determination has been notified by the MEA;

10.2 *The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of:*

a. interest or other earnings due on those accounts, or

b. payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002),

Provided that any such interest, other earnings and payments continue to be subject to those provisions;

11 Regarding 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:

11.1 *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, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.*

11.2 *The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or*

related services have been frozen inadvertently, to the Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

11.3 *The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.*

12 Regarding prevention of entry into or transit through India:

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

12.2 *The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in Foreigners Division of MHA.*

13 Procedure for communication of compliance of action taken under Section 51A:

The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

14 Communication of the Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967:

The order issued under Section 51A of the Unlawful Activities (Prevention) Act, 1967 by the Central [designated] Nodal Officer for the UAPA relating to funds, financial assets or economic resources or related services, shall be communicated to all the UAPA nodal officers in the country, the Regulators of Financial Services, FIU-IND and DNFBPs, banks, depositories/stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties through the UAPA Nodal Officer of the State/UT.

All concerned shall ensure strict compliance of this order.

Annexure- V

Category	Eligible Foreign Investors
I	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II	(a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc. (b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc. (c) Broad based funds whose investment manager is appropriately regulated. (d) University Funds and Pension Funds. (e) University related Endowments already registered with SEBI as FII/Sub Account.
III	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

KYC documents for eligible FPIs under PIS

Document Type		FPI Type		
		Category I	Category II	Category III
Entity Level	**Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)**	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted*	Exempted*	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution @@	Exempted*	Mandatory	Mandatory
Senior	**List**	Mandatory	Mandatory	Mandatory

Management (Whole Time Directors/Partners/Trustee/etc.)	**Proof of Identity**	Exempted*	Exempted*	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted*	Exempted*	Declaration on Letter Head*
	Photographs	Exempted*	Exempted*	Exempted*
Authorized Signatories	**List and Signatures**	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted*	Exempted*	Mandatory
	Proof of Address	Exempted*	Exempted*	Declaration on Letter head*
	Photographs	Exempted*	Exempted*	Exempted*
Ultimate Beneficial Owner (UBO)	**List**	Exempted*	Mandatory (can declare "no UBO over25%)	Mandatory
	Proof of Identity	Exempted*	Exempted*	Mandatory
	Proof of Address	Exempted*	Exempted*	Declaration on Letter Head*
	Photographs	Exempted*	Exempted*	Exempted*

*****Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution'

****