KYC/AML/CFT Policy
(Domestic Branches)
Version No. 14.0
2023-24

S&R Wing
HEAD OFFICE
112, J C ROAD
BENGALURU -560002

INDEX

1. OBJECTIVE

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

a) The objective of KYC/AML/CFT guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering (ML) or Terrorist Financing (TF) activities & to ensure the integrity & stability of the financial system by way of various rules & regulations.

b) Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

c) In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT).

d) In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Bank is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

e) The Reserve Bank of India issues the Directions in accordance with the exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws.

   The provisions of Master Directions, issued by RBI, shall be applicable to Bank.

f) 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.

g) In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002 (15 of 2003). Accordingly, every Bank which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off. The group entities

of the Bank shall put in place mechanism for implementation of the above, in consultation with the Principal Officer of the Bank.

h) KYC policy framework ensures compliance with PML Act/Rules, including regulatory instructions in this regard and provides a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

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.

Explanation- For the purpose of this clause, the terms "Managing Director" & "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

The name, designation & address of the Designated Director shall be communicated to the FIU-IND.

Further, the name, designation, address & contact details of the Designated Director shall also be communicated to the RBI.

In no case, the Principal Officer shall be nominated as the 'Designated Director'.

2.3 Principal Officer:

"Principal Officer" means an officer at the management level nominated by the Bank, responsible for furnishing information under PMLA Rules for the Bank.

The Principal Officer of the Bank shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

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

Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

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 Customer Due Diligence:

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.
Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

2.8 Group:

The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

2.9 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.

2.10 Central KYC Records Registry

In terms of PML rules, "Central KYC Records Registry (CKYCR)" means an entity to receive, store, safeguard and retrieve the KYC records in digital form of a Customer.

2.11 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 10 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 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

(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 10 per cent 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.

2.12 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).

2.13 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.

2.14 Digital KYC

"Digital KYC" means the capturing 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.

2.15 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.

2.16 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.

2.17 Digital Signature:

"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).

2.18 Officially Valid Document:

The Officially Valid Documents are as under:

(1) The Passport.
(2) The Driving License.
(3) Proof of possession of Aadhaar number*.
(4) The Voter's 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 customer submits his proof of possession of Aadhaar number as an Officially Valid Document (OVD), 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 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 carries 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.

2.19 Wealth:

Wealth is the market value of all the tangible & intangible assets (movable or immovable) owned by a person or company or any other entity, as reduced by the debts contracted. Wealth is generally measured through the net worth.

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-III of this Policy.

(iv) Bank will not open an account where the Bank is unable to apply appropriate Customer Due Diligence (CDD) 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 shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer. Bank may also consider closing an existing account under similar circumstances.

(v) Additional information, where such information requirement has not been specified in the internal KYC Policy, is obtained with the explicit consent of the customer.

(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 as mentioned in Point 7, 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).

(xiii) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

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

3.1.1 Risk Perception in respect of Customer:

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

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

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

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

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

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

For this category, higher due diligence is required which includes customer's identity, social/ financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/ services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. 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 identity, social/ financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/ services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. 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 IV of this Policy).

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, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/ services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. 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 IV 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 V – Monitoring of Customer Risk Categorisation (CRC).
   - Submitted Suspicious Transaction Reports (STR) for Customer.
   - Submitted Cash Transaction Report (CTR).
   - Frequent Cheque returns.

D. Risk Categorisation of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer. Example: a Travel Agent (Medium risk) with Proprietorship account (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 categorizing 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.

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 using reliable and independent sources of identification).

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 No. S.O. 3183 (E) 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.

d) The validity period of documents downloaded from CKYCR has lapsed.

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; or

(D) the KYC Identifier with an explicit consent to download records from CKYCR; and

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

(F) 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 as detailed in Annexure IX.

v) KYC Identifier under clause (D) above, the Bank shall retrieve the KYC records online from the CKYCR.

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.

e-KYC services of UIDAI

In case 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/her Aadhaar number, ensure such customer to redacts or blacks out 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.

3.2.3 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.

3.2.4 Accounts of Married Woman:

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

Accordingly, Branches shall accept a copy of marriage certificate issued by the State Government or Gazette notification indicating change in name, together with a verified 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.

3.2.5 Small Accounts:

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

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.

3.2.6 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 2.18 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.

3.2.7 For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the *Bank* may rely on customer due diligence done by a third party; subject to the following conditions:

(a) Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

(b) The Bank takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence

requirements will be made available from the third party upon request without delay;

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

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

(e) The Bank is ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable.

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

The Bank may open accounts using Aadhaar 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.

As a risk-mitigating measure for such accounts, Bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. In case of change of mobile number in accounts opened in non-face-to-face mode using Aadhaar OTP based e-KYC, Branches to ensure that the same is first updated in Aadhaar by the customer before updating in such accounts.

(iii) 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.

(iv) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

(v) 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.

(vi) 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.

(vii) 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.

(viii) 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.

(ix) 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.

3.2.9 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'.
Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (Other than Aadhaar OTP based on-boarding): Non-face-to-face onboarding facilitates the Bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by Bank for non-face-to-face customer onboarding (Other than Aadhaar OTP based on-boarding):

a) V-CIP shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Policy.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

For updation of mobile number in such accounts the following guidelines are to be adhered to:

(i) Register the mobile number after proper verification of the customer's identity.

(ii) Registration/ modification of mobile number is to be made against the customer's written request and only after ascertaining the identity of the customer.

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

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

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

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

3.2.10 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 (v) Accounts of Proprietary Concerns, 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 as per Para No. 3.2.8.

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.

Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Bank.

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 the empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services 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) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Bank. However, in case of call drop / disconnection, fresh session shall be 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 Digi locker.

Bank shall ensure to redact or blackout the Aadhaar number in terms of Para 3.2.2.

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 three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working 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 working 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 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 Digi locker.

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) ***V*-CIP RECORDS AND DATA MANAGEMENT**

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.

3.2.11 Accounts of Foreign students studying in India:

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

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

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

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

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

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

3.2.12 Accounts of Politically Exposed Persons (PEPs)

Bank shall gather sufficient information on any person of this category (whether as customer or beneficial owner) intending to establish a relationship and check all the information available on such person in the public domain & apart from performing normal customer due diligence:

a) Banks should have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP.

b) Reasonable measures are taken by the Banks for establishing the source of funds / wealth.

c) 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.

d) 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 Resources Section (erstwhile MIPD & PP Section) of the respective Regional Office/Circle Office.

e) 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.

f) 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.

Explanation: For the purpose of this Section, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

3.2.13 Accounts of persons other than individuals:

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

(i) Accounts of Companies

Where the client is a company, the certified copies of the 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.
(vii) the names of the relevant persons holding senior management position; and
(viii) the registered office and the principal place of its Business, if it is different.

(ii) Accounts of Partnership firms

Where the client is a partnership firm, the 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.
(v) the names of all the partners, and
(vi) address of the registered office, and the principal place of its Business, if it is different.

(iii) Accounts of Trusts

Where the client is a Trust, the 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.
(v) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the Trust.
(vi) the address of the registered office of the Trust; and
(vii) list of trustees and one copy of an Officially Valid Document containing details of identity and address, one recent photograph and Permanent Account Numbers or Form No.60 for those discharging the role as trustee and authorised to transact on behalf of the Trust.

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

Where the client is an unincorporated association or a body of individuals, certified copies of the 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-documents in the name of the proprietary concern should be submitted as a proof of business/activity:

a) Registration Certificate including Udyam Registration Certificate (URC) issued by the Government.
b) Certificate/license issued by the Municipal authorities under Shop & Establishment Act.
c) Sales and income tax returns.
d) CST/VAT/GST certificate.
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) <u>For opening accounts of a customer who is a juridical person (not specifically covered in the earlier part) such as Societies, Universities and local bodies like Village Panchayats, etc., or who purports to act on behalf of such juridical person or individual or Trust</u>:

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

a) Document showing name of the person authorized to act on behalf of the entity;

b) i) Any Officially Valid Document which contains proof of identity/address in respect of person holding an attorney to transacts on its behalf, and

ii) 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.

c) Such documents as may be required to establish the legal existence of such an entity/juridical person.

Provided that in case of a Trust, the Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as under ::

a. Carrying out any international money transfer operations for a person who is not an account holder of the Bank.

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

c. When a 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 rupees fifty thousand.

(vii) <u>Accounts of Foreign Portfolio Investors (FPIs) for Portfolio Investment Scheme (PIS)</u>:

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 Annexure VIII, 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 Annexure VIII 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.

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

(b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

3.2.15 Accounts of Non Profit Organisations

A Non-Profit Organization (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), 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 (18 of 2013). All transactions involving receipts by these NPOs of value more than Rs.10 lakh 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 lakh; the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal.

3.2.16 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.

3.2.17 Introduction of New Technologies

Bank has to identify and assess the Money Laundering (ML)/ Terrorist Financing (TF) risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, Bank shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

3.2.18 Updation/ Periodic updation of KYC

Periodic Updation means steps taken to ensure that documents, data or information collected under the CDD process as detailed in Para 3.2 is kept up-to-date and relevant by undertaking reviews of existing records 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.

A. CDD requirements for periodic updation:

Banks shall adopt a risk-based approach for periodic updation of KYC ensuring that the documents, information or data collected under CDD process is kept up-to-date and relevant, particularly where there is high risk. 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 through; i) Customer's Email-id/Mobile number registered with the Bank ii) ATM iii) Digital channels (such as Online Banking/ Internet Banking, Mobile Banking) iv) letter.

ii) Change in address:

In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through i) Customer's

Email-id/Mobile number registered with the Bank ii) ATM iii) Digital channels (such as Online Banking/ Internet Banking, Mobile Banking) iv) letter and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification & deliverables.

Branches shall also 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 KYC 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.

iv) Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in accounts opened using Aadhaar OTP based e-KYC in non-face-to-face mode are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Branches shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

(II) ***CUSTOMERS OTHER THAN INDIVIDUALS****:*

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 its email-id registered with the Bank, 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) ***ADDITIONAL MEASURES****:*

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 details, 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.
- The facility of updation of KYC is available at all Branches (including non-home branches) and through Video-Customer Identification Process (V-CIP) if requested by the account holder.
- 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.

(IV) Branches shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship/ account-based relationship and thereafter, as necessary; customers shall submit to the Bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.

B. <u>Temporary ceasing of operations:</u>

In case of existing customers, Bank shall obtain the Permanent Account Number or equivalent e-document thereof 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 equivalent e-documents thereof 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 equivalent e-document thereof 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 equivalent e-document thereof 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.

3.2.19 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.

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

Mule accounts are the crux in fraud supply chain infrastructure and in money laundering process. Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/ illegal money via their Bank account(s).

Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different Bank accounts. They become part of a logistical network that moves money to the pockets of criminals.

Recognizing the significant need and importance of monitoring and identifying suspected mule accounts, our Bank has formed an exclusive Mule Monitoring Team within our Transaction Monitoring Vertical, Operations Wing, HO.

RBI vide its advisory (Frauds/cybercrimes through investment/part time job/Ponzi scheme scams) dated 10/08/2022 has issued detailed guidelines for identification and monitoring of money mule accounts. Any such account, which has been flagged as suspected money mule account, should immediately be subjected to Enhanced Due Diligence (EDD) and enhanced monitoring without any tip-off to the customer. The transactions routed through these identified/suspected money mule accounts should be examined for suspicious transaction reporting to FIU-IND.

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. In such circumstances, Branches/Offices are advised to report transaction details to AML-CFT Centralised Unit, Head Office as per Internal Circular vide No. IC/848/2023.

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, mail/telegraphic transfer/NEFT/IMPS 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.

A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by the Bank.

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 in accounts to ensure their transactions are consistent with Bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

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 customer and closely examine the transactions in order to ensure their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

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, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. 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. The nature and extent of due diligence will depend on the risk perceived by the Bank.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc. may also be used in risk assessment.

Branches shall categorize 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"). Respondent banks may be provided with a wide range of services, including cash / funds management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheques clearing, payable-through-accounts (payable-through-accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf) and foreign exchange services.

In addition to performing normal CDD measures, Bank shall take the following precautions while entering into a cross-border correspondent banking and other similar relationships:

(a) Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank’s business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank’s AML/CFT controls.

(b) The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent

banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.

(c) 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.

(d) Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.

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

(f) Bank shall also ensure that the respondent bank is able to provide the relevant CDD information immediately on request.

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

(h) 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.

(i) Bank shall not enter into a correspondent relationship or continue with a "shell bank" (i.e., a Bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence).

(j) Bank shall ensure that the respondent banks do 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.

Wire transfer related definitions 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** refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

(iii) **Domestic wire transfer** refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.

(iv) **Originator** refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

(v) **Batch transfer:** Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.

(vi) **Beneficiary:** Beneficiary refers to a natural or legal person or legal arrangement who/which is identified by the originator as the receiver of the requested wire transfer.

(vii) **Beneficiary Bank:** It refers to a Bank which receives the wire transfer from the ordering financial institution directly or through an intermediary Bank and makes the funds available to the beneficiary.

(viii) **Cover Payment:** Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

(ix) **Financial Institution***:* In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.

(x) **Intermediary Bank:** Intermediary Bank refers to a Bank which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

(xi) **Ordering Bank:** Ordering Bank refers to a Bank which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

(xii) **Serial Payment:** Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).

(xiii) **Straight-through Processing***:* Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

(xiv) **Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

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 analyzing 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.

A. <u>Information requirements for wire transfers:</u>

i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a. name of the originator;
b. the originator account number where such an account is used to process the transaction;
c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
d. name of the beneficiary; and
e. the beneficiary account number where such an account is used to process the transaction.

In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

ii. In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

iii. Domestic wire transfer, where the originator is an account holder of the ordering Bank, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

iv. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering Bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering Bank and where the information accompanying the wire transfer can be made available to the beneficiary bank and appropriate authorities by other means, it is sufficient for the ordering bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

The ordering Bank shall make the information available within three working/business days of receiving the request from the intermediary Bank, beneficiary Bank, or from appropriate competent authorities.

v. The Bank shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting / competent authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

vi. The wire transfer instructions are not intended to cover the following types of payments:

a) Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the obligation of a Bank to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

B. <u>Responsibilities of ordering bank, intermediary bank and beneficiary bank, effecting wire transfer, are as under</u>:

i. Ordering Bank:

a) The ordering bank shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.

b) Customer Identification shall be made if a customer, who is not an account holder of the ordering bank, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, details to be escalated to AML-CFT Centralized Unit for filing STR with FIU-IND in accordance with the PML Rules.

c) Ordering Bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this section.

ii. Intermediary Bank:

a) Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.

b) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a

related domestic wire transfer, the intermediary bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary bank.

c) Intermediary Bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

d) Intermediary Bank shall have effective risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
(b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iii. Beneficiary Bank*:*

a) Beneficiary Bank shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.

b) Beneficiary Bank shall have effective risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
(b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iv. Money Transfer Service Scheme (MTSS) providers: Bank is required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents.

If Bank controls both the ordering and the beneficiary side of a wire transfer, then it shall:

i. take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

ii. file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

C. <u>Other Obligations</u>:

i. Obligations in respect of Banks' engagement or involvement with unregulated entities in the process of wire transfer.

Bank shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned Bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,

a) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;

b) the agreement / arrangement, if any, with such unregulated entities by Bank clearly stipulates the obligations under wire transfer instructions; and

c) a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

ii. Banks' responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities):

It is prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967 and Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005): Bank shall ensure that it does not process cross-border transactions of Designated Persons and Entities.

iii. Banks' responsibility to fulfil record management requirements:

Complete originator and beneficiary information relating to wire transfers shall be preserved by the Banks involved in the wire transfer in accordance with guidelines of Maintenance, Preservation and Reporting of Customer Account Information as per PMLA Act.

6. MAINTENANCE OF KYC DOCUMENTS AND PRESERVATION PERIOD (RECORD MANAGEMENT)

PML Act and Rules cast certain obligations on the Banks with regard to maintenance, preservation and reporting of customer 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 swiftly to the competent authorities upon request.

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

Explanation – For the purpose of this Section, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

7. COMBATING THE FINANCING OF TERRORISM (CFT)

Branches/CPH are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. Branches/CPH/CPCFT are required to ensure that the names/s of the proposed customer do not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account or processing of SWIFT messages. AML/CFT Centralized 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 and Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.

7.1 Freezing of Assets:

(a) Under Section 51A of Unlawful Activities (Prevention) Act, 1967, in terms of Section 51A of Unlawful Activities (Prevention) Act, 1967 and Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, 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 VI to this Policy) and Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (Annexure VII to this Policy) for ensuring 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. The Director, FIU-India shall be the Central Nodal Officer (CNO) for the Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.

7.2 Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

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

(i) The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html.

(ii) The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.html

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

b. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 (Annexure VI of this Policy).

c. Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annexure VI of this Policy), shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

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

a) Bank shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of

the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annexure VII of this Policy).

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

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

d) In case of match in the above cases, Bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

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

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

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

h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

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

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

C) Bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

Section/Vertical dealing with name screening are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

7.5 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 apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

(b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The processes referred to in (a) & (b) above do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(c) 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. GENERAL GUIDELINES:

8.1 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, or for any other purpose without the express permission of the customer. 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.

8.2 Secrecy Obligations and Sharing of Information:

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

8.3 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.

The foreign contribution should be received only in the exclusive single "FCRA account" of New Delhi Main Branch of SBI (also called designated FC account), as mentioned in the order for registration or prior permission granted and shall be independently maintained by the associations. Besides, this "FCRA Account", the association may also open "another FCRA Account" in any scheduled bank of its choice & link these accounts for transfer of foreign contribution. Also, one or more accounts (called Utilization Account) in one or more scheduled banks may be opened by the association for 'utilizing' the foreign contribution after it has been received in the designated FCRA bank account, provided that no fund other than foreign contribution shall be received or deposited in such account or accounts.

Intimation under rule 9 and rule 17A of the Foreign Contribution (Regulation) Rules, 2011 to the Central Government regarding opening of additional FC-utilization account in respect of the person/association granted registration/ prior permission under the Foreign Contribution (Regulation) Act, 2010 (42 of 2010): in Form FC-6D to be collected and maintained at Branch.

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

8.4 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.

8.5 Need for photographs and address confirmation:

Pass port 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.

8.6 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 for transactions above rupees fifty thousand as required under sub-para (D) of para 3.2.19.

(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 analyze alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers. If Branches/Offices find any transaction or attempted transaction is suspicious, then the same shall be reported to AML-CFT Centralized unit, Head Office as per Internal Circular vide No. IC/848/2023.

(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.

8.7 Issuance of Prepaid Payment Instruments (PPIs):

Bank shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India are strictly adhered to.

****

ANNEXURE- III

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 KYC Identifier with an explicit consent to download records from CKYCR; and **(E)** The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and **(F)** 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 as detailed in Annexure IX. iv) KYC Identifier under clause (D) above, the Bank shall retrieve the KYC records online from the CKYCR. 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) The names of the relevant persons holding senior management position; and (vii) The registered office and the principal place of its business, if it is different. (viii) 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 the 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. (v) The names of all the partners; and (vi) Address of the registered office, and the principal place of its business, if it is different.
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. (v) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust. (vi) the address of the registered office of the trust; and (vii) list of trustees and officially valid documents for those discharging the role as trustee and authorised to transact on behalf of the trust.
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, etc. or who purports to act on behalf of such juridical person or individual or trust.		
		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. Provided that in case of a Trust, the Bank shall ensure that Trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as under: a) Carrying out any international money transfer operations for a person who is not an account holder of the Bank. b) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected. c) When a 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 rupees fifty thousand.
Accounts of Proprietorship Concerns		
	Proof of name, address and activity of the concern	For Proprietary concerns, Customer Due Diligence of the individual (proprietor) is 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 including Udyam Registration Certificate (URC) issued by the Government. b) Certificate/licence issued by the Municipal authorities under Shop & Establishment Act. c) Sales and income tax returns. d) CST/VAT/GST certificate. 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 (c) 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.
Additional documentation for Non-resident Indian along with OVD:		
		A. <u>Proof of Status for NRI/PIO</u> **(1) Proof of NRI status documents (Mandatory for Indian Passport Holder)** Indian Passport with all relevant details along with any one of the below mentioned documents: 1. Valid Visa

		2. Work Permit 3. Proof/certificate of residence 4. Employment /Employment Contract copy 5. Residence Permit 6. E-visa **(2) Proof of PIO status documents (Mandatory for Foreign Passport Holder)** Foreign Passport with all relevant details along with any one of the below mentioned documents: 1. OCI (Overseas Citizen of India) Card 2. PIO (Person of Indian Origin) card 3. Indian Ration Card (Self or Close Relative) 4. Indian Voter ID card (Self or Close Relative) 5. Expired Indian Passport (Self or Close Relative) 6. Marriage Certificate along with spouse's NRI/PIO status proof 7. Certificate issued by Indian Embassy 8. Relevant pages of Passport of Parents / Grand Parents establishing their Indian Origin. **(3) For Seafarer** Indian Passport with all relevant details along with below mentioned documents: 1. Valid Visa 2. Work Permit 3. Valid Job Contract 4. Continuous Discharge Certificate (CDC), if the disembarkation stamp on CDC is not more than 180 months' old 5. Expired contract letter (if the disembarkation stamp on CDC is not more than 180 days' old 6. Pay slips evidencing employment with shipping company (not more than 6 months old) **(4) For Students studying in India (NRO a/c only)** 1. Passport abroad containing identity and address of home country. 2. Valid VISA 3. Immigration Endorsement 4. Admission letter from educational institution 5. Current proof of address within one month of account opening 6. For continuation of account beyond 6 months RBI permission is required (FRRO Registration)

		(5) For Tourists accounts (NRO a/c only) 1. Passport abroad containing identity and address of home country 2. Tourist VISA 3. Immigration Endorsement 4. For continuation of account beyond 6 months RBI permission is required (FRRO Registration) **B. <u>Address Proof Documents Overseas and Indian</u>** **(1) Indian address proof documents (Any one of the below mentioned 1-5)** 1. Indian Passport 2. Aadhaar Card 3. Driving License 4. Voter Identity Card 5. NREGA Job Card signed by officer of state government **(2) Overseas address proof documents (Any one of the below mentioned 1- 20)** 1. Abroad Passport 2. Sale deed agreement 3. Lease deed/rent receipt (mentioning overseas address) not more than 3 months' old 4. Overseas Driving license 5. Company ID containing address 6. ID card issued by government mentioning overseas address (PIO, OCI, Green Card, SSN card issued in US) 7. Utility Bills (Mobile, Water, Electricity, Gas from private or public operators not exceeding 2 months prior only) 8. Employment letter/Employer certificate mentioning overseas address 9. Bank Statement of Overseas Bank account or Indian based bank in abroad (Max.2 months old) 10. Credit card statement mentioning overseas address (Not more than 3 months old from date of application) 11. For Indian Diplomat certificate issued by Indian Diplomatic mission stating correct address 12. Identity Card issued by Foreign government 13. Rent Deed

		14. Government issued letter mentioning overseas address 15. Work Permit mentioning overseas address 16. OCI/PIO card mentioning overseas address 17. NRIs with seafarer work profile and on ship, can either give employer's overseas address or Indian address. 18. Council Tax Bill 19. Permanent Resident permit mentioning overseas address: Example of Resident Permit: UAE- Labor Card, Qatar/Oman/Singapore/Malaysian-Residence card, Saudi Arabia-Resident Permit (Iqama). 20. In case of joint account with close relative, document evidencing and establishing relation is required. **C. Other Important Instructions:** 1. For Overseas Passport Holders Proof of Overseas address should be captured mandatorily. 2. For Indian Passport Holders Overseas address and Indian address should be captured mandatorily 3. Current address shall be overseas only and mandatorily captured 4. Permanent address shall be overseas or Indian address 5. Mailing address shall be Current address or Permanent address as per applicant choice 6. PAN card/Form 60 is mandatory for opening NRO account.
Branches to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.		

ANNEXURE- IV

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

APPENDIX – A

Low Risk	Medium Risk	High Risk
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 20. Corporate 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 the customer is domiciled) 10. Embassies / Consulates

	21. Joint Sector 22. Partnership 23. Private Bank 24. Private Limited Company 25. Unregistered body 26. Proprietorship	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-V

Monitoring of Customer Risk Categorisation (CRC):

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

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

Transactions involving large amounts of cash:

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

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

Transactions that do not make Economic Sense:

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

Activities not consistent with the customer's business:

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

Attempts to avoid reporting/ record- keep requirements:

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

Unusual Activities

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

Customer who provides insufficient or suspicious information

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

Certain suspicious funds transfer activities:

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

ORDER

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

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 Additional Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA [Telephone Number: 011-23092456, 011-230923465 (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.

3.4 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.

3.5 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.

3.6 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.

3.7 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 indicate 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) and any other person:

(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.

(a) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.

(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.

(ix) Any person, either directly or indirectly, holding any funds or other assets of designated individuals or entities, shall, without delay and without prior notice, cause to freeze any transaction in relation to such funds or assets, by immediately informing the nearest Police Station, which shall, in turn, inform the concerned UAPA Nodal Officer of the State/UT along with the details of the funds/assets held. The concerned UAPA Nodal Officer of the State/UT, would follow the same procedure as in para 6.2 to 6.6 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 intention 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;

10.3 (a): The designated individual or organization may submit a request to the Central [Designated] Nodal Officer for UAPA under the provisions of Para 10.1 above. The Central [Designated] Nodal Officer for UAPA may be approached by post at "Additional Secretary (CTCR), North Block, New Delhi – 110001" or through email to jsctcr-mha@gov.in"

(b): The Central [Designated] Nodal Officer for UAPA shall examine such requests, in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and, if accepted, communicate the same, if applicable, to the Ministry of External Affairs, Government of India for notifying the committee established pursuant to UNSC Resolution 1267 (1999) of the intention to authorize, access to such funds, assets or resources in terms of Para 10.1 above.

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.

11A. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/organisations in the event of delisting by the UNSCR 1267 (1999), 1988 (2011) and 1989 (2011) Committee

Upon making an application in writing by the concerned individual/organisation, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs., who in turn shall forward the application along with the full details of the assets frozen to the Central [Designated] Nodal Officer for UAPA within two working days. The Central [Designated] Nodal Officer for UAPA shall examine the request in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and cause such verification as may be required and if satisfied, shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services owned or held by the applicant under intimation to concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs.

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.

15. All concerned are requested to ensure strict compliance of this order.

Annexure – VII

ORDER

Subject: - Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005".

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as 'the Act'] reads as under:

"12A. (1) No person shall finance any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(2) For prevention of financing by any person of any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

a) freeze, seize or attach funds or other financial assets or economic resources—

i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or

ii. held by or on behalf of, or at the direction of, such person; or

iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

II In order to ensure expeditious and effective implementation of the provisions of Section 12A of the Act, the procedure is outlined below.

1. Appointment and communication details of Section 12A Nodal Officers:

1.1 In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for the purpose of this order. [Telephone Number: 011- 23314458, 011- 23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

1.2 Regulator under this order shall have the same meaning as defined in Rule 2(fa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Reporting Entity (RE) shall have the same meaning as defined in Section 2 (1) (wa) of Prevention of Money-Laundering Act, 2002. DNFPBs is as defined in section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.

1.3 The Regulators, Ministry of Corporate Affairs and Foreigners Division of MHA shall notify a Nodal Officer for implementation of provisions of Section 12A of the Act. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act. All the States and UTs shall notify a State Nodal officer for implementation of Section 12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all REs.

2. Communication of the lists of designated individuals/entities:

2.1 The Ministry of External Affairs will electronically communicate, without delay, the changes made in the list of designated individuals and entities (hereinafter referred to as 'designated list') in line with section 12A (1) to the CNO and Nodal officers.

2.1.1 Further, the CNO shall maintain the Designated list on the portal of FIU-India.

The list would be updated by the CNO, as and when it is updated, as per para 2.1 above, without delay. It shall make available for all Nodal officers, the State Nodal Officers, and to the Registrars performing the work of registration of immovable properties, either directly or through State Nodal Officers, without delay.

2.1.2 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other organizations concerned, for initiating verification and suitable action.

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The Bank will maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

2.2 The Nodal Officer for Section 12A in Foreigners Division of MHA shall forward the updated designated list to the immigration authorities and security agencies, without delay.

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

3.1 All Financial Institutions shall –

i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, Bank shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the CNO by email, FAX and by post, without delay.

ii. Run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, Insurance policies etc. In case, the particulars of any of their customers match with the particulars of designated list, Bank 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 on their books to the CNO by email, FAX and by post, without delay.

iii. The Bank shall also send a copy of the communication, mentioned in 3.1 (i) and (ii) above, to State Nodal Officer, where the account/transaction is held, and to their Regulator, as the case may be, without delay.

iv. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A, Bank shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post , without delay.

3.2 On receipt of the particulars, as referred to in Paragraph 3.1 above, the CNO 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 Bank are the ones in designated list and the funds, financial assets or economic resources or related services, reported by Bank are in respect of the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Bank under intimation to respective Regulators. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

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

4.1 The Registrars performing work of registration of immovable properties shall –

i. Verify if the particulars of the entities/individual, party to the transactions, match with the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.

ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. 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 Registrar shall immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.

iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of subsection (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post, without delay.

4.2 the State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.

4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent 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 CNO without delay by email, FAX and by post.

4.4 The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

4.5 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

5. Regarding the real-estate agents, dealers of precious metals/stones (DPMS), Registrar of Societies/ Firms/ non-profit organizations, The Ministry of Corporate Affairs and Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Nodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure 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 shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure 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 State Nodal Officer, without delay.

(iii) The State Nodal Officer 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 or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

(iv) 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 12A, 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

(v) The members of these institutes should also be sensitized by the Institute of Chartered Accountants of India, Institute of Cost and Work Accountants of India and Institute of Company Secretaries of India (ICSI) 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 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(vi) In addition, a member of the ICSI shall, 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, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

(vii) In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure 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 is received,
the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(viii) All communications to Nodal officer as enunciated in subclauses (i) to (vii) above should, inter alia, include the details of funds and assets held and the details of transaction.

(ix) The Other DNBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.

(DNFBPs shall have the same meaning as the definition in Section 2(1) (sa) of Prevention of Money-Laundering Act,2002.)

5.1. All Natural and legal persons holding any funds or other assets of designated persons and entities, shall, without delay and without prior notice, freeze any transaction in relation to such funds or assets and shall immediately inform the State Nodal officer along with details of the funds/assets held, who in turn would follow the same procedure as in para 4.2 to 4.6 above for State Nodal Officer. This obligation should extend to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

5.2 No person shall finance any activity related to the 'designated list' referred to in Para 2.1, except in cases where exemption has been granted as per Para 6 of this Order.

5.3. Further, the State Nodal Officer 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 in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4 Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including Fls and DNFBPs obligated to carry out sanctions screening. The concerned Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

6. Regarding exemption, to be granted to the above orders

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO 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, consequent to notification by the MEA authorizing access to such funds, assets or resources.

This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA to the UNSC or its Committee, and has been approved by the UNSC or its Committee;

6.2. The accounts of the designated individuals/ entities may be allowed to be credited with:

(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 section 12A of the Act.

Provided that any such interest, other earnings and payments continue to be subject to those provisions under para 3.3;

6.3 Any freezing action taken related to the designated list under this Order should not prevent a designated individual or entity from making any payment due under a contract entered into prior to the listing of such individual or entity, provided that:

(i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;

(ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and (iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, he unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization.

7. 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 individual or entity is not a designated person or no longer meet the criteria for designation:

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently

frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

7.2 The RE/Registrar of Immovable Properties/ROC/Regulator and the State Nodal Officer shall inform, and forward a copy of the application, together with full details of the asset frozen, as given by applicant to the CNO by email, FAX and by Post, within two working days. Also, listed persons and entities may petition a request for delisting at the Focal Point Mechanism established under UNSC Resolution.

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it 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 all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

7.4 The CNO shall, based on de-listing of individual and entity under UN Security Council Resolutions, shall pass an order, if not required to be designated in any other order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer.

8. Procedure for communication of compliance of action taken under Section 12A: The CNO 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.

9. Communication of the Order issued under Section 12A: The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

10. This order is issued in suppression of F.No.P-12011/14/2022-ES Cell-DOR, dated 30th January 2023.

11. All concerned are requested to ensure strict compliance of this order.

Annexure- VIII

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 Management (Whole Time Directors/Partners/Trustee/etc.)	**List**	Mandatory	Mandatory	Mandatory
	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'

Annexure – IX

Digital KYC Process

A. The Bank shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Bank.

B. The access of the Application shall be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Bank to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.

D. The Bank must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Bank shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by the Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the Bank shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Bank shall not be used for customer signature. The Bank must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Bank. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Bank, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the Bank shall check and verify that :-

(a) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(b) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the Bank who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

****