KARNATAKA GRAMIN BANK
Head Office, Ballari

KYC POLICY

2025-26

Strategic Planning and Development Wing
HO, Ballari

INDEX

PART-I
GENERAL ASPECTS

1. OBJECTIVES:

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 programmers 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.

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:

- A person or entity that maintains an account and/or has a business relationship with the bank;
- One on whose behalf the account is maintained (i.e. the beneficial owner);
- Beneficiary of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2.2 WALK-IN CUSTOMER:

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

2.3 NON-FACE-TO-FACE CUSTOMERS:

"Non-face-to-face customers" means Customers who open accounts without visiting the branch/offices of the Bank or meeting the Branch Officials.

2.4 POLITICALLY EXPOSED PERSONS (PEPS):

"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.

2.5 NON-PROFIT ORGANISATIONS (NPO):

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).

2.6 DESIGNATED DIRECTOR:

A "Designated Director" means a person designated to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board. The name, designation and address of the Designated Director shall be communicated to the FIU-IND. Further, the name, designation, address and 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'.

2.7 PRINCIPAL OFFICER:

Principal Officer means an Officer **at the management level** nominated by the Bank, responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of thePrincipal 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.

2.8 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 (ito v).
VII. Any agency, office or branch owned or controlled by any of the above persons (i to vi).

2.9 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.

2.10 TRANSACTION:

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

(i) Opening of an account;
(ii) Deposits, withdrawals, 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.

2.11 SUSPICIOUS TRANSACTION:

Suspicious transaction" means a "transaction" as defined below, including an attemptedtransaction, 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 offencespecified 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 tofinance terrorism**.**

2.12 REGULATED ENTITIES:

"Regulated Entities" (REs) means:

a) All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks(LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'Banks'.

b) All India Financial Institutions (AIFIs).

c) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers).

e) All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

2.13 OFFICIALLY VALID DOCUMENTS:

The Officially Valid Documents are as under:

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

*Where the client submits his proof of possession of Aadhaar number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authorityof India (UIDAI).

2.14 AADHAAR NUMBER:

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

2.15 AUTHENTICATION:

"Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

2.16 OFFLINE VERIFICATION:

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

2.17 CENTRAL KYC RECORDS REGISTRY:

"Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

2.18 KNOW YOUR CLIENT (KYC) IDENTIFIER:

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

2.19 KYC TEMPLATES:

"KYC Templates" means templates prepared to facilitate collating and reporting the KYC datato the CKYCR, for individuals and legal entities.

2.20 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 Documentso 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), asdefined 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.

2.21 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, alongwith the latitude and longitude of the location where such live photo isbeing taken by an authorized officer of the Bank.

2.22 DIGITAL SIGNATURE:

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

2.23 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 theprocess. 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.

2.24 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 issuedto 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.

2.25 CUSTOMER DUE DILIGENCE (CDD):

"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 severaltransactions 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, andits 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.

2.26 CUSTOMER IDENTIFICATION:

"Customer identification" means undertaking the process of CDD.

2.27 FATCA:

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

2.28 IGA:

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

2.29 ON-GOING DUE DILIGENCE:

"On-going Due Diligence" means regular monitoring of transactions in accounts to ensure **that those are consistent with Bank's knowledge about the customers, customers' business & risk profile, the source of funds/wealth**.

2.30 PERIODIC UPDATION:

"Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

2.31 SHELL BANK:

"Shell Bank" means 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 andmanagement located within a country. The existence simply of a local agent or low- level staff does not constitute physical presence.

2.32 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).

2.33 PAYABLE-THROUGH ACCOUNTS:

The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

2.34 CORRESPONDENT BANKING:

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 management (e.g., interest- bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable- through accounts and foreign exchange services.

2.35 WIRE TRANSFER RELATED DEFINITIONS:

a) Batch transfer:
Batch transfer is a transfer comprised of a number of individual Wire transfers that are beingsent to the same financial institutions but may/may not be ultimately intended for different persons.

b) Beneficiary:
Beneficiary refers to a natural or legal person or legal arrangement who / which is identifiedby the originator as the receiver of the requested Wire transfer.

c) Beneficiary RE (Regulated Entity):
It refers to a financial institution, regulated by the RBI, which receives the Wire transfer fromthe ordering financial institution directly or through an intermediary RE and makes the fundsavailable to the beneficiary.

d) Cover Payment:
Cover Payment refers to a Wire transfer that combines a payment message sent directly bythe 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 financialinstitution through one or more intermediary financial institutions.

e) Cross-border wire transfer:
Cross-border Wire transfer refers to any Wire transfer where the ordering financial institutionand beneficiary financial institution are located in different countries. This term also refers toany chain of Wire transfer in which at least one of the financial institutions involved is locatedin a different Country.

f) Domestic Wire transfer:
Domestic Wire transfer refers to any wire transfer where the ordering financial institution andbeneficiary 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 systemused to transfer the payment message may be located in another country.

g) Financial Institution:
In the context of Wire-transfer instructions, the term 'Financial Institution' shall have the same meaningas has been ascribed to it in the FATF Recommendations, as revised from time to time.

h) Intermediary RE:
Intermediary RE refers to a financial institution or any other entity, regulated by the RBI whichhandles an intermediary element of the Wire transfer, in a serial or cover payment chain andthat receives and transmits a Wire transfer on behalf of the ordering financial institution andthe beneficiary financial institution, or another intermediary financial institution.

i)Ordering RE:
Ordering RE refers to the financial institution, regulated by the RBI, which initiates the Wire transfer and transfers the funds upon receiving the request for a Wire transfer on behalf of the originator**.**

j) Originator:

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 orderingfinancial institution to perform the Wire transfer.

k) 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).

l)Straight-through Processing:

Straight-through processing refers to payment transactions that are conducted electronicallywithout the need for manual intervention.

m) 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 paymentand settlement system or messaging system used for the Wire transfer.

n) Wire transfer:

Wire transfer refers to any transaction carried out on behalf of an originator through a financialinstitution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and thebeneficiary are the same Person.

2.36 BENEFICIAL OWNER (BO):

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

a) Where the Customer or the owner of the controlling interest is -

(i) an entity listed on a stock exchange in India, or

(ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stockexchanges 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 behalfthey are acting, as also details of the nature of the trust or other arrangements in place shallbe obtained.

2.37. IDENTIFICATION OF BENEFICIAL OWNER:

1. 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-

♦ "Controlling ownership interest" means ownership of / entitlement to more than ***10 per cent*** of the shares or capital or profits of the company.

"Control" shall include the right to appoint majority of the directors or to control themanagement or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

2. 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 percent 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 controlthe management or policy decision.

3. 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 than15 percent 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 (1), (2) or (3) above, the Beneficial owner is the relevant natural person who holds the position of **Senior Managing Official**.

4. Trust:

The identification of beneficial owner(s) shall include identification of the authorof the trust, the trustee, the beneficiaries with 10% or More Interest in the trust and any other natural person exercising ultimate effective control over the trust through achain of control or ownership.

5. Self Help Groups (SHGs) Or Joint Liability Groups (JLGs):

RBI has clarified that the Office Bearers of SHGs/JLGs may deemed to be the Senior Managing Officials. Hence, they shall be treated as Beneficial Owners of SHG/JLG.

3. OBTENTION OF DEEMED OVDs AS PROOF OF ADDRESS:

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 andleave 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 andletter 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 bya marriage certificate issued by the State Government or Gazette notification, indicating sucha change of name.

4. MAINTENANCE OF KYC DOCUMENTS AND PRESERVATION PERIOD:

4.1 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, includingthe following information:

- *The nature of the transactions;*
- *The amount of the transaction and the currency in which it was denominated;*
- *The date on which the transaction was conducted; and*
- *The parties to the transaction.*

4.2 Branches/Offices shall take appropriate steps to evolve a system for proper maintenance, preservation & reporting of **customer information** (with reference to the provisions of PML Act and Rules) in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

4.3 Branches/Offices 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 nature of transactions, the amount of transaction and types of currency involved if any, the date onwhich the transaction was conducted, the parties to the transaction) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity. Transaction details of sale of

third party products and related records shall also be maintained in the similar manner.

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

4.5 Bank shall maintain records of the identity & address of clients, and records in respect of transactions with its clients referred to in Rule 3 of PML Rules 2005, in hard or soft format.

4.6 For the purpose of above, 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.

5. CORRESPONDENT BANKING AND SHELL BANK:

In addition to performing normal CDD measures for approving cross-border correspondent banking and other similar relationships shall be subject to the following conditions:

a) **Bank 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. Bank shall assess the respondent Bank's AML/CFT controls.**

b) **The information gathered in relation to the nature of business of the respondent Bankshall include information on management, major business activities, purpose ofopening 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) Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.

d) **Bank shall clearly document and understand the respective AML/CFT responsibilitiesof institutions involved.**

e) In the case of payable-through-accounts, the correspondent Bank shall be satisfied that therespondent bank has conducted CDD on the Customers having direct access to the accounts**of the correspondent Bank** and is undertaking on-going 'due diligence' on them.

f) The correspondent Bank shall ensure that the respondent Bank is able to provide the relevantCDD information immediately on request.

g) Correspondent relationship shall not be entered into **or continued** with a Shell Bank.

h) It shall be ensured that the **respondent banks** do not permit their accounts to be used by Shell Banks.

i) Banks shall be cautious with **correspondent Banking relationships with institutions** located in jurisdictions which have strategic deficiencies or have not made sufficient progressin implementation of FATF Recommendations.

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

6. WIRE TRANSFER:

A. Information requirements for Wire transfers:

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 thetransaction.
In the absence of an account, a **U**nique **T**ransaction **R**eference **N**umber 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 uniquetransaction 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 RE, 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 RE, 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 isnot an account holder of the ordering RE and where the information accompanying the wire transfer can be made available to the beneficiary RE and appropriate authorities by other means, it is sufficient for the ordering RE 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 RE shall make the information available within three working/business days of receiving the request from the intermediary RE, beneficiary RE, or from appropriate competent authorities.

v) REs 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 / PrepaidPayment 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 ordebit card number or PPI id or reference number accompanies all transfers flowing from thetransaction. 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 an RE to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

B. Responsibilities of ordering RE, intermediary RE and beneficiary RE, effecting Wiretransfer, are as under:

i) Ordering RE:

(a) The ordering RE 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 RE, is intentionally structuring Domestic Wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the Customer, efforts shallbe made to establish identity and if the same transaction is found to be suspicious, STR maybe filed with FIU-IND in accordance with the PML Rules.

(c) Ordering RE shall not execute the wire transfer if it is not able to comply with the requirementsstipulated in this section.

ii) Intermediary RE:

a. RE 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 RE shall keep a record, for at least five years, of all the informationreceived from the ordering financial institution or another intermediary RE.

c. Intermediary RE 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 RE 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 RE:

a. Beneficiary RE shall take reasonable measures, including post-event monitoring or real- timemonitoring 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 lackrequired originator information or required beneficiary information.

b. Beneficiary RE shall have effective risk-based policies and procedures for determining:
(a) when to execute, reject, or suspend a Wire transfer lacking required originator or requiredbeneficiary 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 **and other REs** (Regulated Entities) are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. **REs** that controls both the ordering and the beneficiary side of a Wire transfer shall:

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

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

C. Other Obligations:

i) Obligations in respect of REs' engagement or involvement with unregulated entities in the process of wire transfer:
REs 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 unregulatedentities in the process of wire transfers, the concerned REs shall be fully responsible for information, reporting and other requirements and therefore

shall ensure, inter alia, that,

- There is unhindered flow of complete Wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
- The agreement / arrangement, if any, with such unregulated entities by REs clearly stipulatesthe obligations under Wire transfer instructions; and
- 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) REs' 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):

REs are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Par XI of this Circular, REs shall ensure that they do not process Cross-border transactions of Designated Persons and Entities.

iii) REs' responsibility to fulfill record management requirements:

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

7. JURISDICTIONS THAT DO NOT OR INSUFFICIENTLY APPLY THE RECOMMENDATIONS

a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. **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) fromcountries 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) The background and purpose of transactions with persons (including legal persons and otherfinancial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to ReserveBank/other relevant authorities, on request.

8. COMPLIANCE WITH THE PROVISIONS OF FOREIGN CONTRIBUTION (REGULATION) ACT,2010

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

9. MONEY MULE ACCOUNTS:

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". Money Mules receive cheque deposit or wire transfer and then transfer these funds to accounts held on behalf of another person or other individuals, minus a certain commission.

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).

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules". Banks 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 theBank has not complied with these directions.

A 'Money Mule Account Monitoring Team' has been exclusively formed under Transaction Monitoring Wing, HO in view of recognizing the significant need and importance of monitoring andidentifying suspected 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.

Branches should strictly follow the KYC/AML/CFT Guidelines to prevent abuse of Banking Systemby Money Launderers using Money Mules.

10. OFFICIALLY VALID DOCUMENTS (OVDs):

Officially Valid Documents are those documents that can be accepted for establishing the legal name and current address of the Customer.

The list of such **Officially Valid Documents** are as under:

(a) Passport.

(b) Driving License.

(c) Proof of possession of Aadhaar number.

(d) Voter Identity Card issued by the Election Commission of India.

(e) Job card issued by NREGA (National Rural Employment Guarantee Act) duly

signed by anofficer of the State Government.

(f) Letter issued by the National Population Register (NPR) containing details of name andaddress.

Where the customer submits his proof of Aadhaar number as an OVD, he may submit itin such form as are issued by the Unique Identification Authority of India (UIDAI).

Where OVDs furnished by the Customer does not contain updated address (However, the Customer shall submit updated Officially Valid Document with current address within a period of three months of submitting the said document), the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:

v) Utility bill which is ***not more than two months old*** of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

vi) Property or Municipal tax receipt;

vii) Pension or family pension payment orders (PPOs) issued to retired employees by Government Department or Public Sector Undertakings, if they contain the address;

viii) Letter of allotment of accommodation from employer issued by State Government or CentralGovernment Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licenseagreements with such employers allotting official accommodation.

Where the OVD presented by a **foreign national** does not contain the details of address, insuch 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. **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**.

****

PART-II

CUSTOMER ACCEPTANCE POLICY

"Customer Acceptance Policy" is the first pillar of Know Your Customer and Anti- Money Laundering.

When the documents of identity and address as required under RBI instructions are providedfor KYC compliance, ***Obtention of introduction for opening of accounts is not mandatory***as a part of Customer Acceptance Policy. The accounts opened with proper documents canbe considered as acting in good faith and without negligence by the Bank.

An account will not be opened where the Bank is unable to apply appropriate customer duediligence measures, i.e., unable to verify the Identity &/obtain required documents either dueto non-cooperation of the customer or non-reliability of the documents/information furnishedby the Customer. **The Bank shall consider filing an STR, if necessary, when it is unableto comply with the relevant CDD measures in relation to the customer.** We may also consider closing an existing account under similar circumstances.

Utmost care should be taken while opening new accounts, so as to avoid opening of Benami accounts by unscrupulous persons.

Accounts shall be opened based on Officially Valid Documents only, which will serve as theproof of identity and address of the customer in order to protect the Bank from financial risk.Branch Manager may depute an official to visit the account holder at the given address to satisfy about the genuineness of the address. Verification of trade license, partnership deed,etc., or visit to party's business place will definitely minimize the risk.

Precautions are to be observed to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc., before opening of a new account.

A 'Small Account' means a savings account which is opened in terms of sub-rule (5) **of rule9** of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are as follows:

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

ii. the aggregate of all withdrawals and transfers in a month does not exceed rupeesten thousand; and

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

To open the accounts with relaxed KYC guidelines (titled Small Accounts), the Customer shall produce a copy of the NREGA job card/Aadhaar letter/Self attested photograph & has to sign the account opening form in the presence of the Bank officer who is to certify the same.

Thanks giving letter in NF-154 shall be sent to all the new account holders immediately afteropening of new accounts, which will serve as an address verification process and due diligence measure.

The above is applicable to joint accounts (and also at the time of conversion of individual account to joint account).

****

PART-III

CUSTOMER IDENTIFICATION PROCEDURE

1. Bank shall undertake identification of customers in the following cases:
   i. Commencement of an account-based relationship with the customer.
   ii. Carrying out any international money transfer operations for a person who is not an accountholder of the Bank.
   iii. When there is a doubt about the authenticity or adequacy of the customer identification datait has obtained.
   iv. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupeesfifty thousand.
   v. 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.
   vi. When a RE has reason to believe that a customer (account- based or walk-in) is intentionallystructuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
   vii. REs shall ensure that introduction is not to be sought while opening accounts.

2. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank, may rely on customer due diligence done by a third party, subject to the following conditions:
   i. 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.
   ii. Adequate steps are taken by REs to satisfy themselves that copies of identification data andother relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
   iii. The 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.
   iv. The third party shall not be based in a country or jurisdiction assessed as high risk.
   v. The ultimate responsibility for customer due diligence and undertaking enhanced duediligence measures, as applicable, will be with the Bank.

****

PART-IV

CUSTOMER DUE DILIGENCE PROCEDURE

1. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR INDIVIDUALS:

For undertaking Customer Due Diligence (CDD), Banks 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 andServices) Act, 2016 (18 of 2016);

OR

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

OR

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

OR

(iv) 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 andaddress;

OR

(v) The KYC Identifier with an explicit consent to download records from CKYCR;

AND

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

AND

(C) 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 (AA) 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 theprovisions 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 (AB) above where offlineverification cannot be carried out, the Bank shall carry out verification through digital KYC ***as detailed in Annexure V***.

v) KYC Identifier under clause (AC) above, the Bank shall retrieve the KYC records online fromthe CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government fora 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.

Explanation-1: Bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such Customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) in the previous page.

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.

2. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR SOLE PROPRIETARY FIRMS:

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 shall 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, wouldhave 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 businessactivity has been verified from the address of the proprietary concern.

3. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR COMPANIES:

For opening an account of a Company, certified copies of each of the followingdocuments or the equivalent e-documents thereof shall be obtained:

- Certificate of incorporation.
- Memorandum and Articles of Association.
- Permanent Account Number of the Company.
- A resolution from the Board of Directors and power of attorney granted to its Managers, Officers or Employees to transact on its behalf.
- 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.
- The names of the relevant persons holding Senior Management position; and
- The registered office and the principal place of its business, if it is different.

4. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR PARTNERSHIP FIRM:

For opening an account of a Partnership Firm, the certified copies of each of thefollowing documents or the equivalent e-documents thereof shall be obtained:

- Registration Certificate.
- Partnership Deed.
- Permanent Account Number of the Partnership Firm.
- 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 its behalf.
- The names of all the partners and
- Address of the registered office, and the principal place of its business, if it is different.

5. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR TRUST:

For opening an account of a Trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

1. Registration Certificate.
2. Trust Deed.
3. Permanent Account Number or Form No.60 of the Trust.
4. 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 its behalf.
5. The names of the beneficiaries, trustees, settlor, **protector, if any,** and authors of the Trust.***(A protector is a person who is independent of the trustees. The protector's role is usually to monitor, oversee or control the administration of the trust by the trustees. It is common for a settlor to choose to provide for a protector where a third party/institutional trust company is appointed as trustee).***
6. The address of the registered office of the Trust; and
7. List of trustees and documents, as specified in Point 1, for those discharging the role astrustee and authorised to transact on behalf of the Trust.

6. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR UNINCORPORATED OR BODYOF INDIVIDUALS:

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

1. Resolution of the managing body of such association or body of individuals
2. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
3. Power of attorney granted to transact on its behalf
4. 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 its behalf and
5. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered Trusts / Partnership Firms shall be included under the term'Unincorporated Association'.

Explanation: Term 'Body of Individuals' includes Societies.

7. ACCOUNTS OF JURIDICAL PERSONS (NOT SPECIFICALLY COVERED ABOVE) SUCH AS SOCIETIES, UNIVERSITIES AND LOCAL BODIES LIKE VILLAGE PANCHAYATS ETC., OR WHOPURPORTS TO ACT ON BEHALF OF SUCH JURIDICAL PERSON OR INDIVIDUAL OR TRUST:

For opening account of a Customer who is a Juridical Person (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, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

(i) Document showing name of the person authorized to act on behalf of the entity.

(a) Any Officially Valid Document which contains proof of identity/address in respects ofperson 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 holdinga power of attorney to transact on its behalf.

(ii) 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 whencarrying out transactions as mentioned below:

(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 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 thresholdof rupees fifty thousand.

8. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR LIMITED LIABILITY PARTNERSHIPS (LLP):

(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.
   a. Any Officially Valid Document which contains proof of identity/address in respects ofperson 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 apower of attorney to transact on its behalf.

9. CUSTOMER DUE DILIGENCE (CDD) PROCEDURE FOR SELF HELP GROUPS (SHGs):

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYCnorms 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 SavingsBank 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.

10. ACCOUNTS OF MARRIED WOMAN:

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

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

11. ACCOUNTS OF FOREIGN STUDENTS STUDYING IN INDIA:

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

a) Branches may open a Non-Resident Ordinary (NRO) bank account of a foreign student onthe 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 ofopening 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 foropening the account.

12. ACCOUNTS OF POLITICALLY EXPOSED PERSONS (PEPs) RESIDENT OUTSIDE INDIA:

The Bank shall have the option of establishing a relationship with PEPs (whether as Customer or Beneficial Owner) provided that, apart from performing normal Customer due diligence:

(a) The Bank 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 Bank for establishing the source of funds / wealth;

(c) the approval to open an account for a PEP shall be obtained from theSenior Management;

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

(e) in the event of an existing customer or the beneficial owner of an existingaccount subsequently becoming a PEP, Senior Management's approval is obtained to continue the business relationship;

These instructions shall also be applicable to family members or close associates of PEPs.

"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, seniorgovernment or judicial or military officers, senior executives of state-owned corporations and important political party officials."

13. **Accounts of Non Profit Organizations 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.

14. **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.

15. 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.

16. 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 neither 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. However, Branches/Offices may continue to carry out Customer Due Diligence (CDD) processes in line with regulations governing standards for Know Your Customer (KYC), Anti-Money Laundering (AML), Combating of Financing of Terrorism (CFT)and obligations of regulated entities under Prevention of Money Laundering Act, (PMLA), 2002 in addition to ensuring compliance with relevant provisions under Foreign Exchange Management Act (FEMA) for overseas remittances.

17. ISSUE OF DEMAND DRAFT, ETC. FOR MORE THAN RS.50,000/-.

Any remittance of funds by way of Demand Draft or any other mode and issue of Traveler'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 ofthe 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.

18. 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.

19. AT PAR CHEQUE FACILITY AVAILED BY CO-OPERATIVE BANKS:

Some commercial banks have arrangements with co-operative banks under

which the latteropen 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-operativebanks is in the nature of correspondent banking arrangements, branches maintaining/opening such accounts should monitor and review such arrangements to assessthe 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

20. TEMPORARY CEASING OF OPERATIONS:

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

Provided that before temporarily ceasing operations for an account, the bank shall give the client an accessible notice and a reasonable opportunity to be heard. Further, bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts forcustomers who are unable to provide Permanent Account Number or Form No. 60 owing toinjury, 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 bankgives in writing that he does not want to submit his Permanent Account Number or Form No.60, Bank shall close the account and all obligations due in relation to the accountshall beappropriately 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 purposeof ceasing the operation in the account, only credits shall be allowed.

21. ENHANCED DUE DILIGENCE (EDD) FOR NON-FACE-TO-FACE CUSTOMER ON BOARDING(OTHER THAN CUSTOMER ONBOARDING IN TERMS OF OTP BASED E- KYC A/C OPENING):

Non-face-to-face onboarding facilitates the REs to establish relationship with the Customer without meeting the customer physically or through V-CIP. Such non-face-to- face modes forthe purpose 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 additionalcertifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by Banks for non-face-to-face Customeronboarding (Other than customer onboarding in terms of A/c opening using OTP basede-KYC):

a) In case Bank has introduced the process of V-CIP, the same shall be provided as the first option to the Customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to- face Customer Identification Process.
b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with suchaccounts for transaction OTP, transaction updates, etc. Transactions shall be permitted onlyfrom the mobile number used for account opening. Bank shall have a Board approved policydelineating a robust process of due diligence for dealing with requests for change of registeredmobile number.
c) Apart from obtaining the Current address proof, Bank shall verify the current address throughpositive confirmation before allowing operations in the account. Positive confirmation may becarried 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 verificationfacility of the issuing authority.
e) First transaction in such accounts shall be a credit from existing KYC-complied bank accountof 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 customeris verified in face-to-face manner or through V-CIP.

****

PART-V

MONITORING OF TRANSACTIONS

I. GENERAL ASPECT:

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

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

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

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

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

iii) Transactions involving large amounts of cash inconsistent with the normal and expectedactivity of the Customer.

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

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

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

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

(e) While accepting the cheque for collection, it is to be ensured that the name mentioned in the Challan and name of the Beneficiary of the instrument are same.

(f) Branches are advised to mandatorily obtain either PAN or equivalent e-

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

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

II. COMBATING THE FINANCING OF TERRORISM (CFT)

Branches are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed customer 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.***

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 III to this Policy**) **and Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (Annexure IV 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***.

III. OBLIGATIONS UNDER THE UNLAWFUL ACTIVITIES (PREVENTION) (UAPA) ACT, 1967:

a) Banks 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 toSecurity 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.htm

   Banks 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 Listsand listsas 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 Banks for meticulous compliance

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

c) Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPAOrder dated February 2, 2021 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.

Note: Branches are required to screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed

customer do not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account. AML/CFT Centralised Unit, Head Office will also cross check the details of all existing accounts with the updated list, on a regular basis. If the particulars of any of the account/s have resemblance with those appearing in the list, branches have to verify transactions carried out in such accounts and report those accounts to AML/CFT Centralized Unit, HO for onward submission to RBI/Financial Intelligence Unit-INDIA apart from advising Ministry of Home Affairs as required under UAPA notification dated February2, 2021.

IV. OBLIGATIONS UNDER WEAPONS OF MASS DESTRUCTION (WMD) AND THEIR DELIVERYSYSTEMS (PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005 (WMDACT, 2005):

(a) Banks shall ensure meticulous compliance with the "Procedure for Implementation of Section12A 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 videOrder dated **September 1, 2023**, by the Ministry of Finance, Government of India (Annexedof this Circular).

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

(c) Further, Banks 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 entitiesin 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, Banks shall immediately inform the transaction detailswith 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) Banks may refer to the designated list, as amended from time to time, available on the portalof 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 WMDAct, 2005, Banks 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 Banks from the CNO,Banks 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 shallbe forwarded by Bank along with full details of the asset frozen, as given by the applicant, tothe CNO by email, FAX and by post, within two working days.

(i) Banks shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available athttps://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm , to take into account any modifications to the list in terms of additions, deletionsor 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.

(j) In addition to the above, Banks 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 samefor compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

****

PART-VI

PERIODIC UPDATION

1. DESCRIPTION:

Bank shall adopt a risk-based approach for periodic updation of KYC **ensuring that the information or data collected under Customer Due Diligence (CDD) is kept up-to-dateand relevant, particularly where there is high risk.**

Periodic updation (**Re-KYC**) 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 **tenyears** for **Low risk** customers from the date of opening of the account/last KYC updation. Periodic updation (Re-KYC) can be done at any of our branches.

2. INDIVIDUAL CUSTOMERS:

2.1 In case of change in address:

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

2.2 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) ATMs iii) Digital channels (such as Online Banking/ Internet Banking, Mobile Banking) iv) letter.

2.3 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 ensurethat 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 forwhom account was opened when they were Minor, on their becoming a Major.

2.4 Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. The conditions of account opening using Aadhaar OTP based e-KYC shall not be 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 fromtheaddress in Aadhaar, shall not require positive confirmation in this case. Banks shall ensure that the mobile number for Aadhaar authentication is same as the one available with them inthe Customer's profile, in order to prevent any fraud.

3. CUSTOMERS OTHER THAN INDIVIDUALS:

3.1 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.

3.2 Change in KYC information:

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

4. ADDITIONAL MEASURES:

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

4.1 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.

4.2 Customer's PAN detail, if available with the Branch, is verified from the database of the issuing authority at the time of periodic updation of KYC. Branches shall verify the PAN details in designatedscreen.

4.3 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.

4.4 In order to ensure customer convenience in cases where individual customers express difficulty in approaching the Home Branch due to age related or other issues, such customers may approach theBranch Head or Section in charge of a Non-Home Branch, who shall obtain the necessary KYC documents along with the details as per Bank format from the customer, attest the same and immediately send to the Home Branch for updation in CBS.

4.5 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.

5. Branches shall advise the Customers that in order to comply with the PML Rules, in case of any updatein 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 Branches 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 in CBS.

****

PART-VII

CKYC

CDD PROCEDURE AND SHARING KYC INFORMATION WITH CENTRAL KYC RECORDSREGISTRY (CKYCR):

1. 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 Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November26, 2015.
2. 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.
3. 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.
4. As the CKYCR is now fully operational for individual customers, it has been decided to extendthe 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 Rule9 (1A) of the PML Rules. The KYC records shall be uploaded as per the LE Template released by CERSAI.
5. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Branchesshall 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 KYCinformation is obtained / received from the customer.
6. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Banks shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (3) and (4), respectively, at the time of periodic updation as specified in Part-IV of this Policy, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the RE obtains additional or updated information from any customer as per clause (9) below in this part-VII or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the

concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs a Bank regarding an update in the KYC record of an existing customer, the Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank.

7. 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

8. It is to be ensured that during periodic updation, the customers' KYC details are migratedto current Customer Due Diligence (CDD) standards.
9. For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

(i) there is a change in the information of the customer as existing in the records of CKYCR; or
(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
(iii) the validity period of downloaded documents has lapsed; or
(iv) the Bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

******

PART-VIII

DE-DUPLICATION

(A) REGULATORY GUIDELINES:

- A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual Customers as also the existing Customers.
- The Banks shall, at their option, not issue UCIC to all walk-in/occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who havefrequent transactions with them and ensure that they are allotted UCIC.
- A Unique Customer Identification Code (UCIC) will help the Bank to identify customers, trackthe facilities availed, monitor financial transactions in a holistic manner and enable NPO the Bankto have a better approach to risk profiling of customers.

(B) BANK GUIDELINES:

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.

******

PART-IX
RISK CATEGORISATION

1. DESCRIPTION:

As per RBI Guidelines, Bank shall have a Risk Based Approach (RBA) for **mitigation & management of the risks (identified on their own or through national risk assessment)**which includes the following:

- Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Bank.
- FATF Public Statement, the reports and guidance notes on KYC/AML issued by the IndianBanks Association (IBA) may also be used in risk assessment.
- A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
- **The Bank shall implement a CDD programme, having regard to the ML/TF risks identified and the size of the business.**

2. RISK CATEGORIZATION OF CUSTOMERS:

Based on the policy/guidance notes of RBI/IBA, risk rating has been assigned taking intoaccountthe 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.

Note:

- The review of risk categorization of customer's accounts and updation thereof (Wherever necessary) is being carried out **on daily basis with a periodicity of six months betweeneach review**.
- Final risk categorization shall be done taking into consideration the rating in all the seven parameters.

Low Risk customers (Level 1 Customers):
Individuals (Other than High Networth) and entities whose identities and sources of income canbe easily identified and transactions in whose accounts by and large conform to the known profiles may be categorized 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 requirement 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 categorizedas medium or high risk
For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, sources of funds and his/her client profile, etc.besides proper identification.
An indicative list of Medium Risk Customers is as under:

- Gas Dealers
- Car/boat/plane dealers
- Electronic(Wholesale)
- Travel agencies
- Telemarketers
- Telecommunication Service Provider
- Pawnshops
- Auctioneers
- Restaurants, Retail shops, Movie theaters, etc.
- Sole practitioners
- Notaries
- Accountants
- Blind
- Purdanashin

High Risk Customers (Level 3 Customers):

For this category, higher due diligence is required which includes customer's background, natureand location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank shall subject such accounts to enhanced monitoring on an ongoing basis. Anindicative 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 ultimatebeneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers.
- High Networth Individuals*
- Non Residents Customers.
- Accounts of Cash intensive business 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).

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 whiletaking into account the above aspects. For instance, a salary class individual who is generallyto be classified under low risk category may be classified otherwise based on the perceptionof 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 I of this note).

Customer Risk Categorization

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 finalize parameters which are available in the system and the same shall be reviewed annually. System shall assign provisional risk categorization based onthe 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 clients business and their location etc. The nature of due diligence will depend on the risk perceived by the Bank. Risk categorization shall be donebased on selected parameters and assigning suitable risk category.

Risk Parameters

The first step in process of risk categorization is selected of parameters, which would determinecustomer risk.

IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation ofBanks 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. Country of Residence/Nationality: Whether India or any overseas location/Indian or foreignnational.
3. Product Subscription: salary account, NRI products etc.

4. Economic profile: HNI, public Ltd. Company etc.
5. Account status: Active, incorporative, dormant.
6. Account Vintage: Less than six months old etc.
7. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.
8. Suspicious Transaction Report (STR) filed for the customer.
9. AML alerts.

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

Risk Rating of Customers:

Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending onbackground, 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 I** of this Note.

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

Account Types	**High**	**Medium**	**Low**
Only SB*	Rs.200000/-& above	Rs. 100000/-& above but less than Rs 200000/-	Less than Rs. 100000/-
Only Current*	Rs.500000/-& above	Rs. 200000/- &above but less than Rs 500000/-	Less than Rs. 200000/-
Only Term Deposits	Rs.1000000/-& above	Rs. 500000/- &above but less than Rs 1000000/-	Less than Rs. 500000/-

* applicable to accounts which have completed 6 months

** For current/SB accounts balance amount and for Term deposits, principle amount shall be taken for consideration on the date of review.
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 neednot be clubbed for the above purpose.

a. 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 II- Monitoring of

Customer RiskCategorization (CRC).

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

b. Risk categorization 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 Saving account with average balance of Rs 1,50,000/- and Term Deposit of Rs 4,00,000/- (Low risk), shall be assigned with overall ratingof 'Medium Risk', provided all other conditions mentioned under C above does not necessitatefor 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 Categorization provided by the SP&D Wing (as detailed under points A,B,C & D above), risk ratinghas been assigned taking into account the following parameters available in CBS system :

- Customer constitution
- Customer profession
- Type of Business
- Product code
- Account status
- Account Vintage
- Average balance in deposit in SB/Current/Term Deposit accounts.

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

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 willnot identify the customers/accounts named in complaints (from legal enforcement authorities)/frauds, this parameter has not been included in the Risk Categorization Matrix. Branches are advised to categorize such customers/accounts under "High Risk" category as andwhen complaints from legal enforcement authorities) are received or fraud is reported against the customer/account holder.

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

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

Under vintage parameter, newly opened CASA accounts which have not completed 6 months shall be categorized as High Risk, except accounts pertaining to staff, ex-staff, pensioners, small accounts, Financial Inclusion and Basic Saving 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 to be takeninto 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 aftertwelve months subject to complying with other parameters.

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

Roles and Responsibilities of Branches:

Branches shall review Customer risk categorization based on the risk categorization generated by the system, every six months, as on 15th May and November every year. Branches may also apply addition alert indicators to address specific risks faced by them.

Roles and responsibilities of Regional Offices:

- Shall monitor/follow-up process of review/classification/re-classification of CustomerRisk Categorization.
- Shall ensure compliance of Risk Categorization at branches every six months byobtaining confirmation from branches.
- Shall submit periodical reports on implementation/review of risk categorization to SP&DWing, H.O
- Shall attend/follow-up audit observation/remarks.

SP&D Wing, H.O

- Oversee implementation/monitoring and review of risk categorization of customers byputting in place suitable reporting/monitoring mechanism.
- Ensure proper maintenance of MIS for customer risk categorization and migration data.
- Shall review fixing of parameters available through the system annually
- SP&D Wing along with PMO, shall identify the parameters available in the system forrisk categorization through the system as per model suggested in the policy.
- Shall review and provide necessary recommendations/directions to strengthenadherence of KYC/AML guidelines.

Inspection Wing, HO

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

Monitoring/Review of Customer Risk Categorization (CRC):

Branches shall carry out a review of risk categorization of customers at a periodicity of not less than once in six months i.e., as on 15th of May and November every year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.
Wherever there is suspicion at branch level that a Customer is above low risk, branches should carry out customer due diligence (CDD).

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

- Customer locations
- Financial Status
- Nature of Business
- Purpose of transaction

OTHER GUIDELINES:

- 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 legalenforcement authorities)/frauds, this parameter has not been included in the Risk Categorization Matrix. Branches are advised to categorize such Customer ID under "High Risk" category as and when complaints (from legal enforcement authorities) are received or fraud is reported against the Customer/Account holder.
- Accounts of dealers in Jewelry, gold/silver/bullions, diamonds and other precious metals/stones shall be categorized under High Risk.
- The review of risk categorization of customer's accounts and updation thereof (Wherever necessary) shall be carried out on daily basis with a periodicity of six month. During such review, the risk assigned to an existing Customer may undergo change depending on the change in risk parameters of the Customer. Wherever there is suspicion at Branch level thata Customer is above low risk, Branches should carry out Customer Due Diligence (CDD).
- Branches shall review Customer risk categorization based on the risk categorizationgenerated by the system, every six months i.e., 30th Jun and 31st December every year and submit the periodical report to their respective RO. Branches may also apply additionalalert indicators to address specific risks faced by them. Further, RO shall submit periodical reports on implementation/review of risk categorisation to SP&D wing, Head Office, Ballari.

******

PART-X

VIDEO BASED CUSTOMER IDENTIFICATION PROCESS (VCIP)

Regulatory Guidelines:

An alternate method of customer identification with facial recognition and Customer Due Diligenceby 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 throughindependent 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

Bank may undertake V-CIP to carry out:

- Customer Due Diligence (CDD) in case of new customer on-boarding for individualcustomers, 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 Part IV, apart from undertaking CDD of the Proprietor.
- Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.
- Updation/Periodic updation of KYC for eligible customers.

2. V-CIP INFRASTRUCTURE:

2.1 The Bank should have complied with the RBI guidelines on minimum baseline cyber securityand 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 transferredto 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 serviceprovider or third-party technology provider assisting the V-CIP of the Bank.

2.2 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.

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

2.4 The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customerundertaking 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.

2.5 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.

2.6 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 asa cyber-event under extant regulatory guidelines.

2.7 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 encryptioncapabilities. Any critical gap reported under this process shall be mitigated before rolling outits implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

2.8 The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance and strength before being usedin 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 conformitywith internal/ regulatory guidelines.

3. VCIP PROCEDURES:

3.1 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.

3.2 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 multiplefiles, 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.

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

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

3.4 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.

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

- OTP based Aadhaar e-KYC authentication.
- Offline Verification of Aadhaar for identification.
- KYC records downloaded from CKYCR, in accordance with Para VII, using the KYC identifier provided by the customer.
- 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 Section 16. In caseof offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the dateof carrying out V-CIP.

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, Bank shall ensure that the video process of the V-CIP is undertaken withinthree 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.

3.6 If the address of the customer is different from that indicated in the OVD, suitable records ofthe 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.

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

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

3.9 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.

3.10 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.

3.11 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.

3.12 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.

4. V-CIP RECORDS AND DATA MANAGEMENT:

4.1 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 andbears 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.

****

PART-XI

REPORTING REQUIREMENTS

(a) <u>Reporting to Financial Intelligence Unit-India</u>

1.1. In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by Non-Profit Organisations (NPO) [NPO means any entity or organisation , 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 required 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)], cash transactions where forged or counterfeit currency notes or Bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit- India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

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

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

1.4. In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Branches/ Offices/ Sections shall take note of the timeliness of the reporting requirements and submit the reports within the timelines. Bank shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

1.5. Bank, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information.

under Point 1 (1.1) (g) of this Policy of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

And also where Bank is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, the CDD process shall not be pursued, and instead file an STR with FIU-IND.

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

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

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

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

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

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

(b) <u>Reports to be furnished to FIU-IND:</u>

1. CASH TRANSACTION REPORTS (CTR):

The Bank shall scrupulously adhere to the following:

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

1.2 While filing CTR, details of individual transactions below Rupees Fifty Thousand need not befurnished.

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

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

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

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

2. SUSPICIOUS TRANSACTION REPORTS (STR)

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

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

2.3 No account is opened where the Bank is unable to apply appropriate CDD measures, eitherdue to Non-Cooperation of the Customer or non-reliability of the documents/ information furnished by the Customer. **The Bank shall consider filing an STR, ifnecessary, when it is unable to comply with the relevant CDD measures in relation to the customer.**

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

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

2.6 In the context of creating KYC/AML awareness among the staff and for generating alerts forsuspicious transactions, Branches may consider the indicative list of suspicious activities contained in KYC Policy of the Bank.

2.7 Bank shall not put any restrictions on operations in the accounts **merely on the basis of STR filed**. **The Bank & their employees shall ensure that the fact of maintenance of records referred to in PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirementshall not inhibit sharing of information of any analysis of transactions and activities which appear unusual, if any such analysis has been done.**

3. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT BY BANK:

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

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

(b) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. Further, the periodicity of risk assessment exercise shall be determined by the Board **or anycommittee of the Board** of the Bank **to which power in this regard has been delegated**, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

4. NON-PROFIT ORGANISATION (NPO):

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

5. COUNTERFEIT CURRENCY REPORT (CCR):

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

6. CROSS-BORDER WIRE TRANSFER REPORT:

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

As per recent amendments to Prevention of Money Laundering (PML) Rules, every reporting entity is required to maintain the record of all transactions including the

record of all cross borderwire transfers of more than Rs.5 lakh or its equivalent in foreign currency, where either the originor destination of the fund is in India. The information shall be furnished electronically in the FIN-Net module developed by FIU-IND.

(c) Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

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

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

"Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

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

a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login - -> My Account --> Register as Reporting Financial Institution,

b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to. Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

f) Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following:
   - Updated Guidance Note on FATCA and CRS
   - A press release on 'Closure of Financial Accounts' under Rule 114H (8).

****

Disclaimer:

Review of the KYC Policy of the Bank Policy for the Financial Year 2025-26:

Any mandated additions as per guidelines from NABARD, RBI, DFS, Sponsor Bank, or any other regulatory bodies, as well as subsequent amendments or modifications communicated post- adoption, seamlessly integrate into this Policy. The Bank is committed to complying with all additional policy requirements as they arise.

Validity of the Policy:

This policy comes in to effect immediately and shall be valid until the next review and adoptionof policy by the by the Board of Directors

****

ANNEXURE- I

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-II

Monitoring of Customer Risk Categorisation (CRC):

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

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

Transactions involving large amounts of cash:

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

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

Transactions that do not make Economic Sense:

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

Activities not consistent with the customer's business:

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

Attempts to avoid reporting/ record- keep requirements:

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

Unusual Activities

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

Customer who provides insufficient or suspicious information

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

Certain suspicious funds transfer activities:

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

Annexure-III

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 Governmentshall 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 inthe Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

c. prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

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

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

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

3. Appointment and communication details of the UAPA Nodal Officers:

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated]Nodal Officer for the UAPA [Telephone Number: 011-23092456, 011- 230923465 (Fax), emailaddress: jsctcr-mha@gov.in].

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of

3.3 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 andcommunicate the name and contact details to the Central [designated] Nodal Officer for theUAPA.

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 theUN sanction measures whenever changes are made in the lists by the UNSC 1267 Committeepertaining 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 thechanges 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 withoutdelay.

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 thereal 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 givenparameters 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) aboveto the UAPA Nodal Officer of the State/UT where the account is held and to Regulators andFIU-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 heldby 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 areheld for the benefit of the designated individuals/entities, an orders to freeze these assetsunder Section 51A of the UAPA would be issued by the Central [designated] nodal officerfor 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 economicresources 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. 011-23092551and also convey over telephone No. 011-23092548. The particulars apart from being sent bypost 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 StatePolice 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 ofthe verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.

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

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

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

7. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and otherDesignated 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 theconcerned 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 dealershould 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 inturn 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 andinform 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 transactionand without delay inform the CBIC, who in turn follow the similar procedure as laid down inthe 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 UAPANodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laiddown 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 Casinoand/ 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 Casinoowner 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 respectivemembers to the provisions of Section 51A of UAPA, so that if any designated individual/entityapproaches 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 arrangedfor 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 thesimilar 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 registeredwith 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 orlimited 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 Ministryof 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 designatedindividuals 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 PoliceStation, which shall, in turn, inform the concerned UAPA Nodal Officer of the State/UT alongwith 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.SecurityCouncil 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, terroristacts 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 behalfof, 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 andassociated 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 Resolution1373, 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 examinedwithout 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 suspector 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 shallbe 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 UAPAto be:-

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, orexclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routineholding 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 suchnotification;

(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 onwhich 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 thoseprovisions;

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 Ministryof External Affairs, Government of India for notifying the committee established pursuant toUNSC 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 theUAPA 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 detailsof the asset frozen given by any individual or entity informing of the funds, financial assetsor 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 theconcerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurancecompany, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA NodalOfficer 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/organization, 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 forUAPA 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, theUAPA 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 individualswhose 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 Officerof the State/UT.

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

To,

1) Governor, Reserve Bank of India, Mumbai
2) Chairman, Securities & Exchange Board of India, Mumbai
3) Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4) Foreign Secretary, Ministry of External Affairs, New Delhi.
5) Finance Secretary, Ministry of Finance, New Delhi.
6) Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7) Secretary, Ministry of Corporate Affairs, New Delhi
8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9) Director, Intelligence Bureau, New Delhi.
10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
11) Chief Secretaries of all States/Union Territories
12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13) Directors General of Police of all States & Union Territories
14) Director General of Police, National Investigation Agency, New Delhi.
15) Commissioner of Police, Delhi.
16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance,New Delhi.
18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19) Director (FIU-IND), New Delhi.

Copy for information to: -
1. Sr. PPS to HS
2. PS to SS (IS)

Annexure-IV

ORDER

Subject: - Procedure for implementation of Section 12A of "The Weapons of MassDestruction 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 Actfor 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 underthis Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act forthe 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 CentralGovernment 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 orrelated 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 deliverysystems.

(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), E mailaddress: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 theAct. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementationof 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 Section12A 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 Nodalofficers.

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 2.1above, without delay. It shall make available for all Nodal officers, the State NodalOfficers, 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 REs 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 theupdated designated list to the immigration authorities and security agencies, without delay.

3. Regarding funds, financial assets or economic resources or related servicesheld 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, REs 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 relationwith a customer and on a periodic basis to verify whether individuals and entitiesin the designated list are holding any funds, financial assets or economicresources or related services, in the form of bank accounts, stocks, Insurancepolicies etc. In case, the particulars of any of their customers match with the particulars of designated list, Res shall immediately inform full particulars of thefunds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books tothe CNO by email, FAX and by post, without delay.

iii. The REs 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, andto 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 Section12A, REs 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 CentralAgencies so as to ensure that the individuals/entities identified by the REs are the ones in designated list and the funds, financial assets or economic resourcesor related services, reported by REs 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 freezethese assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned RE 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/ Commissionersof 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 immovableproperties:

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, matchwith the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particularsof 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 givenparameters, 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, andif 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 beconveyed, 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. Thisverification 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 freezethese 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 CNOshall also forward a copy thereof to all the PrincipalSecretaries/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 CorporateAffairs 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 underclause (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 delayand 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 to4.6.

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensurethat 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 transactionfor 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 laiddown 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 designatedindividual/ 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 Section12A, 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 themember 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 shouldnot 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.

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 Officerin the Ministry of Corporate Affairs, who shall follow the similar procedure as laiddown 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.

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 PartnershipFirm 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 fundsor assets of the designated individual/ entity, he shall follow the similar procedureas 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 firmshall 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 CorporateAffairs.

(vi)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.

(vi) 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 andassets 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 personsor 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 personsor 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 / accountsof 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 attemptsby 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, FinancialInstitutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including FIs 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 oreconomic resources that have been determined by the CNO to be: -

- 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 notificationby 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.

- necessary for extraordinary expenses, provided that such determination hasbeen notified by the MEA to the UNSC or its Committee, and has been approvedby the UNSC or its Committee;

6.3 The accounts of the designated individuals/ entities may be allowed to be creditedwith:

- Interest or other earnings due on those accounts, or
- 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 theAct.

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

6.4 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:

- 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;

- 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 NodalOfficer.

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 thedetails 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 underSection 12A of the Act by the CNO relating to funds, financial assets or economicresources 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 30thJanuary 2023.

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

(Manoj Kumar
Singh)Director
(HQ)

To,

1) Governor, Reserve Bank of India, Mumbai
2) Chairman, Securities & Exchange Board of India, Mumbai
3) Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4) Foreign Secretary, Ministry of External Affairs, New Delhi.
5) Finance Secretary, Ministry of Finance, New Delhi.
6) Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7) Secretary, Ministry of Corporate Affairs, New Delhi
8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9) Director, Intelligence Bureau, New Delhi.
10) Additional Secretary, Department of Financial Services, Ministry of Finance,NewDelhi.
11) Chief Secretaries of all States/Union Territories
12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13) Directors General of Police of all States & Union Territories
14) Director General of Police, National Investigation Agency, New Delhi.
15) Commissioner of Police, Delhi.
16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17) Joint Secretary (Capital Markets), Department of Economic Affairs, MinistryofFinance, New Delhi.
18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, NewDelhi.
19) Director (FIU-IND), New Delhi.

Copy for information to: -

1. Sr. PPS to HS
2. PS to SS (IS)

Annexure-V

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.

****