KNOW YOUR CUSTOMER (KYC) –
ANTI MONEY LAUNDERING (AML) POLICY

Document Name:	Know Your Customer (KYC) - Anti Money Laundering (AML) Policy
Version Number:	15.0
Prepared & Owned By:	Operation Department, HO
Reviewed & Approved By:	BOM & BODs
Recommended in BOM Dated	16 June, 2025
Approved in BOD Meeting Dated:	21 June, 2025
Released Date	21 June, 2025

Sr. No.	Date of Revision / Review	Version Number	Released & Distributed To
1.	21 June, 2025	15.0	All Branches & All Departments Head Office/PRO/ HODC
2.	15 March, 2025	14.0	
3.	26 November, 2024	13.0	
4.	24 March, 2024	12.0	
5.	30 January, 2024	11.0	
6.	18 November, 2023	10.0	
7.	27 May, 2023	9.0	
8.	11 February, 2023	8.0	
9.	09 July, 2022	7.0	
10.	12 June, 2021	6.0	
11.	27 June, 2020	5.0	

12.	23 July, 2019	4.0	
13.	27 May, 2018	3.0	
14.	15 May, 2016	2.0	
15.	Sept. 2014	1.0	

REFERENCE OF RBI DIRECTIONS			
Master Direction	25th February, 2016	RBI/DBR/2015-16/18 Master Direction DBR. AML.BC. No. 81/14.01.001/2015-16	Master Direction – Know Your Customer (KYC) Directions, 2016

INDEX

CHAPTER – I

PRELIMINARY

1. Title, Commencement and Objective

(a) This policy shall be called as Know Your Customer (KYC) and Anti Money Laundering (AML) Policy, which is duly approved by Board.

(b) This policy shall come into effect immediately.

(c) India, being a member of Financial Action Task Force (FATF) is committed to upholding measures to protect the integrity of the international financial system. To prevent Bank from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of various rules and regulations. The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:

i) To prevent Bank from being used intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.

ii) To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank's Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

iii) The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

iv) For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

2. Scope of Policy and Applicability

2.1 All branches of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s). The policy is applicable across all branches / offices of the Bank and is to be read in conjunction with related policy guidelines issued from time to time.

2.2 The contents of this policy shall be subject to the changes / modifications which may be advised by RBI and / or any other regulators / or by bank from time to time.

3. Definitions

In policy, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

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

ii. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii. **"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.

iv. Beneficial Owner (BO)

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

Explanation: For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

b. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.

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

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

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

is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. "Certified Copy" – Obtaining a certified copy by regulated entity shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the regulated entity as per provisions contained in the Act.

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

- Authorized officials of overseas branches of Scheduled Commercial Banks registered in India.
- Branches of overseas banks with whom Indian banks have relationships.
- Notary Public abroad,
- Court Magistrate.
- Judge.
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

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

vii. **"Designated Director"** means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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

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

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

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

xi. **"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).

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

xiii. **"Non-profit organizations"** (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).

xiv. **"Officially Valid Document"** (OVD) means the passport, the driving license, Proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

a) Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b) Where the OVD furnished by the customer does not have updated address, the following documents or equivalent e-documents thereof shall be deemed to be 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, postpaid 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 Departments or Public Sector Undertakings, if they contain the address.

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

c) The customer shall submit OVD with current address within a period of three months of submitting the documents specified at "(b)" above

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

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

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

Definition of Offline Verification:

Offline verification is defined as a process of verifying the identity of an individual through offline modes. The modes for offline verification have not been specified and left upon Unique Identification Authority of India (UIDAI) to specify, by means of regulations.

During offline verification, the branches / bank must:

i. Obtain the consent of the individual,

ii. Inform them of alternatives to sharing information, and not to collect, use or store Aadhaar number or biometric information.

xvi. "Person" has the same meaning assigned in the Act and includes:

a. an individual,

b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvii. Deleted from RBI directions

xviii. "Principal Officer" means an officer at the management level nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

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

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

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

xx. A **'Small Account'** means a savings account which is opened in terms of sub rule (5) of rule 9 of the PML Rules 2005. Details of the operation of a small

account and controls to be exercised for such account are specified in section 23.

xxi. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of an account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
    - any payment made or received, in whole or in part, for any contractual or other legal obligation; or
e. establishing or creating a legal person or legal arrangement.

(b) Terms bearing meaning assigned in this Policy, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. **"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.

ii. **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.

iii. **"Customer"** means a person who is engaged in a financial transaction or activity with Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

v. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

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

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

vi. **"Customer identification"** means undertaking the process of CDD.

vii. **"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.

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

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

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

xi. **"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 and risk profile, the source of funds / wealth.

xii. **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

xiii. **"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 reviewsof existing records at periodicity prescribed by the Reserve Bank.

xiv. "**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) Asset Reconstruction Companies (ARCs)

(e) All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instruments Issuers (PPI issuers)

(f) All Authorized Persons (APs) including those who are agents of Money Transfer Scheme (MTSS), regulated by the Regulator.

Our Bank being UCB, is a 'Regulated Entity' as per above definition.

xv. **"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 and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

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

xvii. **"Wire transfer"** related definitions

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

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

(c) Beneficiary bank: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary bank and makes the funds available to the beneficiary.

(d) Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the

cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

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

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

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

(h) Intermediary bank: Intermediary bank refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

(i) Ordering bank: Ordering bank 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 ordering financial 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 electronically without 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 payment and 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 financial institution 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 the beneficiary are the same person.

(c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act,2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II

GENERAL

4. Policy Name & Approval Authority

(a) The present policy is a Know Your Customer (KYC) / Anti Money Laundering (AML) Policy of the Bank, which is duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.

(b) 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 programs 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 programs shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

(c) Bank's policy framework shall seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, Bank may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

5. Key Elements

This KYC policy includes following four key elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures (CIP); and

(d) Monitoring of Transactions

5A. Money Laundering and Terrorist Financing Risk Assessment by Bank:

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

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with 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 any committee 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 Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

(d) Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. Bank shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Bank shall monitor the implementation of the controls and enhance them if necessary.

6. Designated Director

(a) A “Designated Director” means a person designated by the bank nominated by the Board, 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.

(b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(c) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

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

7. Principal Officer

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

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

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

8. Compliance of KYC policy

(a) Bank shall ensure compliance with KYC Policy through roles and responsibilities of various departments and sections with regard to KYC/AML/CFT matters which are as below.

(i) Operations & N.I.D. Department:

To issue guidelines regarding KYC/AML/CFT for domestic deposits and implementation/monitoring of the same, including liaison with RBI/IBA/FIU/other agencies, reporting to regulatory authorities apart from attending/monitoring STR/CTR and CCR alerts. Various reports shall be collated by Accounts Department on behalf of the Principal Officer.

(ii) I.T. Department:

To give technology support for implementation of the policy/directions from regulator and for compliance of legal framework in the matter, e.g. AML, e-KYC, CKYCR etc., as required from time to time.

(iii) Inspection Department:

To arrange to include necessary templates in audit program for verification of implementation of KYC/AML/CFT guidelines through Concurrent Audit and Internal Inspection and shall submit Compliance Report to Audit Committee monthly/quarterly.

(b) Bank shall not outsource the decision-making functions of determining compliance with KYC norms.

CHAPTER – III

CUSTOMER ACCEPTANCE POLICY

9. Bank's Customer Acceptance Policy is as follows.

Bank shall develop clear Customer Acceptance Policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the Bank.

10. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, Bank shall ensure that:

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

(b) No account is opened where the Bank is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

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

(d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.

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

(f) Bank shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a bank desires to open another account or avail any other product or service from the same bank, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

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

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

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

11. Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

As per RBI/2015-16/61 dated 1st July, 2015 Master Circular on Customer Service – UCBs it is directed to include 'third gender' in all forms / application etc. wherein any gender classification is envisaged. Bank shall follow the guidelines in this regard and has inserted the same in CIF forms.

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system. In Core Banking System we already have a unique Customer ID (Cust ID). This Cust ID is allotted to every customer while entering into any new relationship, which will serve as the Unique Customer Identification Code (UCIC). The banking relationship of customer includes relationship such as Depositor, Borrower,

Guarantor, Regular/Nominal Member, etc., The banking relationship guideline is also applicable to a walk-in customer who doesn't have an account with our bank and he/she request for Pay Order or Banker's cheque for amount below Rs. 50,000/-

However, there can be cases where the customer has been allotted multiple Cust IDs since the bank was not informed about his/her existing customer ID. For such customers the multiple customer IDs has been consolidated and one of the Cust ID has been maintained as the active UCIC.

11A. Where bank forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

CHAPTER – IV

RISK MANAGEMENT

12. For Risk Management, Bank shall have a risk based approach which includes the following.

(a) Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception.

(b) Broad principles may be laid down by the bank for risk-categorization of customers.

(c) Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

(d) The risk categorization of a customer and the specific reasons for such

categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc., has been used in risk assessment. Guidance note on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all Urban Co-Operative Banks by the RBI etc., has been used in risk assessment exercise.

12A. Risk categorization of Customers:

"Customer risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from Bank's perspective. This risk is based on risk perceptions associated with customer profile.

RBI has directed that Banks are required to prepare a Risk profile of each customer and apply enhanced due diligence measures on High risk customers. As per IBA working group guidelines, Banks 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.

(I) Low Risk Customers

Individuals (other than High Net worth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as Low Risk customers.

Updating KYC of Low Risk Customers: Every 10 years.

(II) Medium Risk Customers

Customers who are likely to pose a higher than average risk to the branch/CPC should be categorized as medium or high risk.

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

Updating KYC of Medium Risk Customers: Every 8 years.

(III) High Risk Customers

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Branch/CPC shall subject such accounts to enhanced monitoring on an ongoing basis.

Updating KYC of High Risk Customers: Every 2 years.

Bank shall adopt manual classification. Based on the availability of data, Bank shall finalize parameters which are available in the system and the same shall be reviewed as and when required. **Branches shall make suitable modification/revision, if need be, based on remaining indicators as covered in the policy**.

For categorizing a customer as low risk, medium risk and high risk, the parameters considered are location of customer and his client, mode of payments, nature of activity, volume of turnover and social and financial status. **The indicative list of Low, Medium and High Risk customers are given in Table A.**

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

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, risk rating has been assigned taking into account the following parameters available in CBS system:

1. Customer type
2. Profession of Customer
3. Type of Business
4. Product Code
5. Account Status
6. Account Vintage

Table – A	**List of Low/Medium/High Risk Type of Customers**
Low Risk	
1)	Co-operative Bank
2)	Ex-staff, Govt./ Semi Govt. Employees
3)	Illiterate Individual
4)	Individual
5)	Local Authority / Local Body
6)	Other Banks
7)	Pensioner
8)	Private / Public Sector Bank
9)	Private Ltd. Company
10)	Proprietorship
11)	Public Ltd. Company
12)	Public Sector Co/Corp.
13)	Senior Citizen
14)	Self Help Group
15)	Staff

Medium Risk	
1)	Auctioneers
2)	Blind
3)	Car / Boat / Plane Dealership
4)	Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theatres, etc.

5)	Corporate Body
6)	Dot-com Company or Internet Business
7)	Electronics (Wholesale)
8)	Gas Station/Petrol pumps
9)	Joint Venture
10)	Notaries
11)	Pardanashin
12)	Partnership Firm
13)	Pawnshops
14)	Providers of telecommunications service, internet cafe, IDD call service, phone cards, phone center
15)	Register Body
16)	Secretarial Firms
17)	Sole Practitioners or Law Firms
18)	Telemarketers
19)	Travel Agency
20)	Used Car Sales
21)	Venture Capital Companies

High Risk	
1)	Accounts under Foreign Contribution Regulation Act
2)	Association of Persons/Clubs
3)	Bullion dealers and jewellers (subject to enhanced due diligence)
4)	Business accepting third party cheque (except supermarkets or retail stores that accept payroll cheque / cash payroll cheque
5)	Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.
6)	Companies having close family shareholding or beneficial ownership
7)	Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale

8)	Customers based in high risk countries / jurisdictions or locations
9)	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.
10)	Customers engaged in a business which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries
11)	Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
12)	Customers that may appear to be Multi-Level marketing companies etc.
13)	Customers with dubious reputation as per public information available or commercially available watch lists
14)	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)
15)	Embassies / Consulates
16)	Executors / Administrators/HUF
17)	Firms with 'sleeping partners'
18)	Gambling/gaming including “Junket Operators” arranging gambling tours
19)	High Net Worth individuals.
20)	Import/ Export
21)	Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs
22)	Individuals and entities in watch lists issued by Interpol and other similar international organizations
23)	Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
24)	Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention

25) Investment Management / Money Management Company / Personal Investment Company
26) Minor
27) Money Service Business, including seller of Money Orders / Travelers' Cheque / Money Transmission / Cheque Cashing / Currency Dealing or Exchange
28) Non face-to-face Customers
29) Non-Banking Financial Institutions
30) Non-resident Customers and foreign nationals having average annual credit turnover over Rs.10.00 lacs
31) Off-shore (foreign) Corportaion/Business
32) Politically exposed persons (PEPs)
33) Pooled Accounts
34) 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
35) Stock Broker
36) Trusts, charities, NGOs/NPOs (especially those operating on a "cross- border" basis)

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

In addition to this, the categorization mentioned above will be allocated to the customers at the time of account opening & might get changed on half yearly basis derived from the parameters defined for risk categorization

While reviewing and calculating customer risk categorization on half yearly basis, Customer IDs belonging to entities such as HUFs, Trusts, Jewellers, Builders, AOPs, Clubs, Co-op. Housing Societies, PEPs and Minors will retain their classification under High Risk category, without alteration.

12B. Change in Customer Risk categorization after filing STR:

Customer will be flagged as high risk in CBS on the same day after filing/submitting Suspicious Transaction Report (STR) to FIU-IND, ensuring this customer's risk rating remains effective for the subsequent two years, as this is a crucial step in managing Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) risks. After completing period of two years, the said customer will be re-categorized based on the parameters defined for risk categorization.

(a) Risk Mitigation:

Filing STR indicates suspicion of illegal activity associated with a particular customer or transaction. Marking the customer as high risk ensures that the bank applies enhanced due diligence measures to mitigate the risks associated with that customer. Consequently, increased monitoring of transactions, more frequent reviews of the customer's activity, and additional verification procedures should be done meticulously.

(b) Regulatory Compliance:

Regulatory authorities require banks to assess and manage the risks associated with their customers, particularly those identified as high risk due to suspicious activities. By marking the customer as high risk, the bank demonstrates compliance with AML and CTF regulations, which mandate the implementation of appropriate risk-based measures to prevent financial crime.

(c) Preventing Further Transactions:

Marking a customer as high risk alerts the bank's compliance and risk management teams to closely scrutinize any further transactions involving that customer. This helps to prevent the customer from using the bank's services to conduct additional suspicious activities while the investigation is ongoing.

(d) Protecting the Bank's Reputation:

Failing to adequately address risks associated with suspicious transactions or customers can damage a bank's reputation and expose it to regulatory penalties.

By promptly marking high-risk customers and implementing appropriate risk management measures, banks demonstrate it's commitment to combating financial crime and protecting their reputation as responsible financial institutions.

(e) Effective Monitoring and Reporting:

Marking a customer as high risk facilitates ongoing monitoring and reporting of their activities, ensuring that any subsequent suspicious transactions are promptly identified and reported to the relevant authorities. This contributes to the overall effectiveness of the bank's AML and CTF compliance efforts.
In essence, the process of marking a customer as High Risk in the CBS, post STR filing is vital for comprehensive risk management, regulatory adherence, safeguarding bank's reputation & thwarting financial crime. It enables bank to implement appropriate risk-based measures and enhance their ability to detect and report suspicious activities.

CHAPTER – V

CUSTOMER IDENTIFICATION PROCEDURE (CIP)

13. Bank shall undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer, i.e. at the time of opening of any type of account.
(b) Carrying out any international money transfer operations for a person who is not an accountholder of the bank.
(c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
(d) Selling third party products as agents, selling our own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand. (presently bank is not issuing credit cards, prepaid/travel cards)
(e) 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.

(f) When the Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(g) Bank shall not seek introduction while opening accounts.

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, **Bank shall not use services of third party.**

CHAPTER – VI

CUSTOMER DUE DILIGENCE (CDD) PROCEDURE

Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

15. Deleted from RBI directions.

16. For undertaking CDD, bank shall obtain the following from an individual while establishing an account based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

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

(ii) he decides to submit his Aadhaar number voluntarily to a bank or any bank notified under first proviso to sub-section (1) of section 11A of the PML Act; or

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

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

(ac) 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 / 61 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 notified under first proviso to sub-section (1) of section 11A of the PML Act, 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 the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Bank shall carry out verification through digital KYC as specified under Annex I.

v) KYC Identifier under clause (ac) above, the bank shall retrieve the KYC records online from the CKYCR in accordance with paragraph 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the Bank 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.

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or equivalent e-document from customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in paragraph 8. Bank shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackouts his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank officials/Business Correspondent/Business Facilitators.

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

17. Accounts opened using OTP based e-KYC, in non-face to face mode are subject to the following conditions: ***(At present, bank is not allowing accounts opened using OTP based e-KYC, in non-face to face mode, hence this para. Shall no be exercised)***

i. There must be a specific consent from the customer for authentication through OTP.

ii. As a risk-mitigating measure for such accounts, bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Bank shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.

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

v. As regards borrower accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per paragraph 16 or as per paragraph 18 (V-CIP) is carried out, If Aadhaar details are used under paragraph 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrower accounts no further debits shall be allowed.

viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face- to- face mode with any other Bank / Regulated Entities as defined under sub-section (b) xiii of section 3 of this policy. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Banks / Regulated Entities, shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face to face mode.

ix. Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

18. Bank may undertake V-CIP to carry out:

(At present, Bank has not opted V-CIP, hence this option shall not be exercised.)

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

Provided that in case of CDD of a proprietorship firm, bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm,as mentioned in paragraph 28 and paragraph 29, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per paragraph 17.

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

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

(a) V-CLIP Infrastructure

i) The bank should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the bank only and all the data including video recording is transferred to the RE's exclusively owned / leased server(s)

including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the bank.

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

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

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

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

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

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/regulatory guidelines.

(b) V-CIP Procedure

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

ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the bank. However, in case of call drop / disconnection, fresh session shall be initiated.

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

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

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

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

the following:

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with paragraph 56, using the KYC identifier provided by the customer

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

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

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

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

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

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

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

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

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

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

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

(c) V-CIP Records and Data Management

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

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

19. Deleted from RBI directions.

20. Deleted from RBI directions.

21. Deleted from RBI directions.

22. Deleted from RBI directions.

23. Notwithstanding anything contained in paragraph 16 and as an alternative thereto,

in case an individual who desires to open a bank account, banks shall open a 'Small Account' which entails the following limitations

I. The aggregate of all credits in a financial year does not exceed rupees one lakh:

II. The aggregate of all withdrawal's and transfers in a month does not exceed rupees tenthousand; and

III. The balance at any point of time does not exceed rupees fifty thousand.

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

Further small accounts are subject to the following conditions:

(a) The bank shall obtain a self-attested photograph from the customer.

(b) The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

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

(c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

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

(e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months ofthe opening of the said account.

(f) The entire relaxation provisions shall be reviewed after twenty-four months.

(g) The account shall be monitored and when there is suspicion of money

laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per paragraph 16.

(h) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per paragraph 16 or paragraph 18.

24. Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs) : (paragraph 24 is not applicable to the Bank)

25. Deleted from RBI directions

26. KYC verification once done by one branch of the Bank shall be valid for transfer of the account to any other branch, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Part II - CDD Measures for Sole Proprietary firms

27. For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

28. In addition to the above, any two of the following documents or the equivalent e-documents thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

I. Registration certificate including Udyam Registration Certificate (URC) issued by the Government
II. Certificate/license issued by the municipal authorities under Shop and Establishment Act
III. Sales and income tax returns
IV. CST/VAT/ GST certificate (provisional/final)
V. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
VI. IEC (Importer Exporter Code) issued to the proprietary concern by the office

of DGFT/ License /certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute

VII. 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.

VIII. Utility bills such as electricity, water, and landline telephone bills.

29. In cases where the bank is satisfied that it is not possible to furnish two such documents, Bank may, at its discretion, accept only one of those documents as proof of business/activity.

Provided Bank undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Note: RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s).

Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.

Part III- CDD Measures for Legal Entities

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

I. Certificate of incorporation

II. Memorandum and Articles of Association
III. Permanent Account Number of the company
IV. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
V. Documents, as specified in paragraph 16 relating to beneficial owner, the managers, officersor employees as the case may be, holding an attorney to transact on its behalf
VI. The names of the relevant persons holding senior management position; and
VII. The registered office and the principal place of its business, if it is different.

31. For opening an account of a **partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

I. Registration certificate
II. Partnership deed
III. Permanent Account Number of the Partnership firm
IV. Documents as specified in paragraph 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
V. The names of all the partners and
VI. Address of the registered office, and the principal place of its business, if it is different.

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

I. Registration certificate
II. Trust deed
III. Permanent Account Number or Form No.60 of the trust
IV. Documents, as specified in paragraph 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding a power of attorney to transact on its behalf
V. The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust

VI. The address of the registered office of the trust; and

VII. List of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorized to transact on behalf of the trust.

33. **A.** 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:

(a) Resolution of the managing body of such association or body of Individuals

(b) Permanent Account Number or Form No.60 of the unincorporated association or body of individuals

(c) Power of attorney granted to transact on its behalf

(d) Documents, as specified in paragraph 16, relating to beneficial owner, managers, officers or employees ,as the case may be holding an attorney to transact on its behalf and

(e) Such information as may be required by the Bank 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.

B. For opening account of **a customer who is a juridical person** (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

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

(b) Documents as specified in paragraph 16 of the person holding an attorney to transact on its behalf and

(c) Such documents as may be required by the bank to establish the legal existence of such anentity/juridical person.

Provided that in case of a trust, the Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of paragraph 13 of this policy.

Part IV - Identification of Beneficial Owner

34. 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:

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

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

Part V - On-going Due Diligence

35. Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with bank's knowledge about the customers, customers' business and risk profile; the source of funds / Wealth.

36. Without prejudice to the generality of factors that call for close monitoring following types oftransactions shall necessarily be monitored:

I. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
II. Transactions which exceed the thresholds prescribed for specific categories of accounts.
III. High account turnover inconsistent with the size of the balance maintained.
IV. Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

37. The extent of monitoring shall be aligned with the risk category of the customer.

(a) 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 as under.

Review of Risk Categorization of the customers shall be done according to the risk perceived while taking into account the following 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" or "Medium Risk" such as:

- Unusual transaction/ behavior
- Submitted Suspicious Transaction Reports (STR) for Customer
- Reported under Cash Transaction Report (CTR)
- For the purpose of review of risk rating loan accounts, term deposits, shareholders and S.D.Locker holders are to be excluded for considering relationship vintage and credit turnover in account as the turnover is routed through **checking accounts** by the customer.
- The regularity or duration of the relationship will be given due weightage.

Long standing relationship involving frequent customer contact throughout the relationship may be considered less risk from the money laundering perspective.

To facilitate review on above lines, Points no. i, ii, iii & iv of para No 4.4.5 of Guideline Note on the subject matter circulated vide RBI communication No. UBD.BPD (PCB) Cir. No. 57/14.01.062/2013-14 Dt. May 6, 2014 have been taken into consideration. As per these guidelines the risk assessment should take into account risk variables specific to a particular customer or transaction, which includes the level of transactions to be deposited by customers or size of transactions undertaken. It suggests that low level of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow for treating the customer as lower risk. It further also indicates that the regularity or duration of the relationship be considered. Long standing relationship involving frequent customer contact throughout relationship present less risk from money laundering perspective.

Keeping in view these guidelines contained in above referred RBI communication dated 6thMay 2014 risk categorization of accounts be reviewed on the parameters mentioned herein below. Customers moved to higher risk categories i.e. High Risk and Medium Risk categories upon risk review shall retain same higher risk category for subsequent two year seven if their risk category is lowered during subsequent reviews.

If Existing Risk Category is Low

Vintage	Annual Credit Turnover	Risk Category
Up to 3 yrs.	Above Rs.24 Lakh to Rs.60 lakh	Medium
Up to 3 yrs.	Above Rs.60 Lakh	High
Above 3 yrs. up to 10 yrs.	Above Rs.60 Lakh up to Rs.120 Lakh	Medium
Above 3 yrs. up to 10 yrs.	Above Rs.120 Lakh	High
Above 10 yrs.	Above Rs.120 Lakh up to Rs.180 Lakh	Medium
Above 10 years	Above Rs.180 Lakh	High

If Existing Risk Category is Medium

Vintage	Annual Credit Turnover	Risk Category
Up to 3 yrs.	Up to Rs.24 Lakh	Low
Up to 3 yrs.	Above Rs.60 Lakh	High
Above 3 yrs. up to 10 yrs.	Up to Rs.60 lakh	Low
Above 3 yrs. up to 10 yrs.	Above Rs.120Lakh	High
Above 10 yrs.	Up to Rs.120 Lakh	Low
Above 10 yrs.	Above Rs.180 Lakh	High

If Existing Risk Category is High

Vintage	Annual Credit Turnover	Risk Category
Up to 3 yrs.	Up to Rs.24 Lakh	Low
Up to 3 yrs.	Above Rs.24 Lakh to Rs.60 lakh	Medium
Above 3 yrs. up to 10 yrs.	Up to Rs.60 lakh	Low
Above 3 yrs. up to 10 yrs.	Above Rs.60 Lakh up to Rs.120 Lakh	Medium
Above 10 yrs.	Up to Rs.120 Lakh	Low
Above 10 yrs.	Above Rs.120 Lakh up to Rs.180 Lakh	Medium

(b) The transactions in accounts of marketing firms, especially accounts of Multi-Level Marketing (MLM) Companies shall be closely monitored.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

38. Updation / Periodic Updation of KYC

Bank shall adopt a risk-based approach for periodic updation of KYC ensuring

that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of bank's internal KYC policy duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.

Notwithstanding the provisions given above, in respect of an individual customer who is categorized as low risk, the bank shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The bank shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

a) Individual Customers:

i. **No change in KYC information**: In case of no change in the KYC information, a self- declaration from the customer in this regard shall be obtained through customer's email- id registered with the RE, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc.

ii. **Change in address**: In case of a change only in the address details of the customer, a self- declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, bank at their option, may obtain a copy of OVD, as defined in paragraph 3(A)(xiv) or deemed OVD or the equivalent e-documents thereof, as defined in paragraph 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of updation / periodic updation. Such requirement, however, shall be clearly specified by the bank in their internal KYC policy duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.

iia. **Use of Business Correspondent (BC) by banks for Updation/ Periodic Updation of KYC:** Self-declaration from the customer in case of no change in KYC information or change only in the address details may be obtained through an authorized BC of the bank. The bank shall enable its BC systems for recording these self-declarations and supporting documents thereof in electronic form in the bank's systems.

The bank shall obtain the self-declaration including the supporting documents, if required, in the electronic mode from the customer through the BC, after successful biometric based e-KYC authentication. Until an option is made available in the electronic mode, such declaration may be submitted in physical form by the customer. The BC shall authenticate the self-declaration and supporting documents submitted in person by the customer, and promptly forward the same to the concerned bank branch. The BC shall provide the customer an acknowledgment of receipt of such declaration /submission of documents.

The bank shall update the customer's KYC records and intimate the customer once the records get updated in the system, as required under paragraph 38(c) of the Master Direction ibid. It is, however, reiterated that the ultimate responsibility for periodic updation of KYC remains with the bank concerned.

(Currently, the bank doesn't offer KYC Updation through Business Correspondents (BCs). The Bank will adhere to RBI guidelines pertaining to BCs as and when the service is implemented.)

iii. **Accounts of customers who were minor at the time of opening account on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the bank. Whereverrequired, bank may carry out fresh KYC of such customers i.e. customers for whom accountwas opened when they were minor, on their becoming a major.

iv. Aadhaar OTP based e-KYC in non-face to face mode may be used for updation / periodic updation. To clarify, conditions stipulated in paragraph 17 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

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

b) Customers other than individuals:

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

ii. **Change in KYC information:** In case of change in KYC information, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

c) Additional Measures: In addition to the above, bank shall ensure that,

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

ii. Customer's PAN details, if available with the bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation / 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.

iv. In order to ensure customer convenience, banks may consider making available the facility of updation / periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.

v. Bank shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the bank such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.

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

e) Due Notices for Periodic Updation of KYC: The bank shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the bank shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the RE shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder shall be duly recorded against each customer for audit trail. The bank shall expeditiously implement the same but not later than January 01, 2026.

39. Freezing and closure of Non-KYC Compliance Accounts:

(a) It would be always open to Bank to close the account of KYC non-complaint customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision need to be taken by the Branch Manager.

While it is absolutely necessary for banks as well as customers to comply with the measures prescribed for KYC/AML purposes, drastic measures like closing of accounts may be taken only after sending out sufficient discernible warning

signals to the customers, basing on the level of customer education and public awareness on the subject. In all such cases where the account holders are either not responding over a period of time/not found at the given address, Bank may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

Before taking the extreme step of closing an account on account of non-compliance with the KYC/AML requirements, as an initial measure, branches are advised to place such accounts under close watch, depriving the non-compliant customers certain additional facilities, till the customer complies with such requirements.

In case of non-compliance of KYC requirements by the customers despite repeated reminders by branches, branches should impose “partial freezing” on such KYC non-compliant accounts in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force.

While imposing “partial freezing”, branches are advised to ensure that the option of “partial freezing” is exercised after giving due notice of three months initially to the customers to comply with KYC requirements and followed by a reminder for further period of three months. Thereafter, branches to impose “partial freezing” by allowing all credits and disallowing all debits, with the freedom to close the accounts.

If the accounts are still KYC non-compliant after six months of imposing initial “partial freezing”, branches should disallow all debits and credits from/to the accounts, rendering them inoperative.

If the customer despite such measures, shows unwillingness to comply with KYC/AML/CFT requirements, it would always be open to the branches to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken by the Branch Manager.

Before closure of such account, branch shall send a notice to the nominee/legal heirs of the account holder, if registered with the bank.

In the Circumstances when the Bank believes that it would no longer be satisfied about the true identity of the account holder, the Bank shall file a Suspicious Transaction Report (STR) with Financial Intelligence Unit India (FIU-IND) under the Department of Revenue, Ministry of Finance, and Government of India.

Example:

1st Notice regarding Compliance of KYC:	**01/01/2023**
2nd Notice cum Reminder regarding Compliance of KYC:	**01/04/2023**
Debit Freeze the Account on:	**01/07/2023**
(1) Issue a final notice regarding closure of account & Total Freeze the account on:	**01/01/2024**
(2) Also a notice to nominee regarding closure of account of nominator on:	**01/01/2024**
Closure of Account on:	**01/04/2024**

(b) In case of existing customers, Bank shall obtain Permanent Account Number or the equivalent e-documents thereof or Form No. 60 by such date as may be notified by the Central Government, failing which Bank will temporarily cease operations in the account till the time the permanent Account Number or e-equivalent document thereof or Form No.60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank will give the client an accessible notice and a reasonable opportunity to be heard. Further, in case customers who are unable to provide Permanent Account Number or the equivalent e-documents thereof or Form No 60 owing to injury, illness or infirmity on account of old age or otherwise necessary supporting proofs for such inability shall be obtained by the branches to allow appropriate relaxation for continued operation of accounts from Operations Department, Head Office. Accounts where such relaxation is granted shall be

subject to enhanced monitoring.

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

Explanation: For the purpose of this paragraph, "temporary ceasing of operations" in relation an account will 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 provision of this paragraph. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account only credits will be allowed.

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

40. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17):
(At present bank doesn't open accounts of non-face to face customers)

Non-face-to-face onboarding facilitates the bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be

undertaken by bank for non- face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17):

a) In case bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Bank shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
c) Apart from obtaining the current address proof, bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

41. Accounts of Politically Exposed Persons (PEPs)

A. 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:

I. Bank have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

II. Reasonable measures are taken by the REs for establishing the source of funds / wealth;

III. The approval to open an account for a PEP is taken at a senior level at Operations Department at Head Office.

IV. all such accounts are subjected to enhanced monitoring on an on-going basis;

V. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, approval from Operations Department at head Office is obtained to continue the business relationship;

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

Explanation: For the purpose of this Paragraph, "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.

42. Client accounts opened by professional intermediaries:

Bank shall ensure while opening client accounts through professional intermediaries, that:

(a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

(b) Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

(c) Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.

(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of bank, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of bank, the bank shall look for the beneficial owners.

(e) Bank shall, at its discretion may rely on the 'customer due diligence' (CDD) done by an intermediary which is regulated, and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

(f) The ultimate responsibility for knowing the customer lies with the bank.

B. Simplified Due Diligence

43. Simplified norms for Self Help Groups (SHGs)

(a) CDD of all the members of SHG shall not be required while opening the saving bank account of the SHG

(b) CDD of all the office bearers shall suffice

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

44. Procedure to be followed by banks while opening accounts of foreign students

As UCBs are not authorized to open NRO accounts, no account of any foreign student shall be opened by the bank.

45. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Considering various restrictions/permissions required for such type of accounts, at present no account of any foreign portfolio investors shall be opened by the bank.

CHAPTER VII
RECORD MANAGEMENT

46. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Bank shall,

I. maintain all necessary records of transactions between the bank and the customer, both domestic and international, for at least five years from the date of transaction;

II. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

III. make available the identification records and transaction data to the competent authorities upon request;

IV. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

V. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
   (I) the nature of the transactions;
   (II) the amount of the transaction and the currency in which it was denominated;
   (III) the date on which the transaction was conducted; and
   (IV) the parties to the transaction.

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

VII. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

Explanation: For the purpose of this Paragraph, 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.

46A. Bank shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the bank has ended or the account has been closed, whichever is later.

CHAPTER VIII
REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA

47. Bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the bank for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

48. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by bank. (made available by FIU-IND on its website http://fiuindia.gov.in.)

49. While furnishing information to the Director, FIU-IND, delay of each day in not

reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts merely on the basis of the STR filled.

Every 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 Paragraph 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

50. AML software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

CHAPTER IX

REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES

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

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

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

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

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

II. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

III. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967: The procedure laid down in the UAPA Order 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 Ministry of HomeAffairs (MHA).

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

(a) Bank shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India.

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

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

(d) In case of match in the above cases, bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Bank shall file an STR with FIU- IND covering all transactions in the accounts, covered above, carried through or attempted.

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

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

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Bank shall prevent such individual/entity from conducting financial transactions, under intimation to

the CNO by email, FAX and by post, without delay.

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

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

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

53A. In addition to the above, Bank shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

53B. Bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

54. Jurisdictions that do not or insufficiently apply the FATF Recommendations

I. 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) from countries for which this is called for by the FATF.

II. 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.

III. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

54A. Bank is encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

CHAPTER X
OTHER INSTRUCTIONS

55. Secrecy Obligations and Sharing of Information:

I. Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
II. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged

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

III. While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

IV. The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of bank requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

55A. 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 to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

56. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

(a) Bank 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 authorized 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 No. S.O. 3183(E) dated November 26, 2015.

The Bank shall upload the KYC data pertaining to all new individual accounts on or after from April 1, 2017 with CERSAI in terms of the

provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

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

(c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(d) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

(e) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Scheduled Commercial Banks (SCBs)/ Cooperative Banks are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. SCBs were initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017.

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

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

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

bank obtains additional or updated information from any customer as per clause (j) below in this paragraph 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 an 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.

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

(j) For the purposes of establishing an account based relationship, updation/ periodic updation or for verification of identity of a customer, the RE 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.

57. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, Bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether it is 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: Banks shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

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

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

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

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following:

i. updated Guidance Note on FATCA and CRS

ii. a press release on 'Closure of Financial Accounts' under Rule 114H

58. Period for presenting payment instruments

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

59. Operation of Bank Accounts & Money Mules

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

60. 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.

61. (a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into newrelationships with individual customers as also the existing customers by bank.

(b) The bank shall, at its option, not issue UCIC to all walk-in/occasional customers (such as buyer of pre-paid instruments/purchasers of third party products) provided it is ensured that there is adequate mechanism to identify

such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

62. Introduction of New Technologies

(Debit Cards/Credit Cards/ Smart Cards/Gift Cards/Mobile Wallet/Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.)

Adequate attention shall be paid by Bank to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/ technologies. Bank shall identify and assess the ML/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.

63. Correspondent Banks

(At present bank does not have any Correspondent Bank)

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent banking and other similar relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

I. Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has

been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.

II. The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.

III. 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.

IV. Bank shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.

V. In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent 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.

VI. The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.

VII. Correspondent relationship shall not be entered into or continued with a shell bank.

VIII. It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.

IX. Banks shall be cautious of correspondent banking relationships with institutions located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

X. 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.

64. Wire transfer

(At present, terms related to domestic wire transfer are only applicable to our bank)

A. Information requirements for wire transfers for the purpose of this Master Direction:

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

a. name of the originator;

b. the originator account number where such an account is used to process the transaction;

c. the originator's address, or national identity number, or customer identification number, or date and place of birth;

d. name of the beneficiary; and

e. the beneficiary account number where such an account is used to process the transaction.

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

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

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

iv. Domestic wire transfers of rupees fifty thousand and above, where the

originator is not an account holder of the ordering bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

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

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

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

vi. The wire transfer instructions are not intended to cover the following types of payments:
    a. Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

    b. Financial institution-to-financial institution transfers and settlements,

where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

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

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

i. Ordering Bank:

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

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

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

ii. Intermediary Bank:

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

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

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

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

d. Intermediary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iii. Beneficiary Bank:

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

b. Beneficiary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

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

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 to determine 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 bank's engagement or involvement with unregulated entities in the process of wire transfer

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

i) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
ii) the agreement / arrangement, if any, with such unregulated entities by bank clearly stipulates the obligations under wire transfer instructions; and
iii) 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. Bank's 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)

Bank is prohibited from conducting transactions with designated persons

and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, bank shall ensure that they do not process cross-border transactions of designated persons and entities.

iii. **Bank's responsibility to fulfil record management requirements**

Complete originator and beneficiary information relating to wire transfers shall be preserved by the bank involved in the wire transfer, in accordance with paragraph 46 of the Master Direction.

65. Issue and Payment of Demand Drafts, etc.,

Any remittance of funds by way of demand draft, mail/telegraphic transfer/ NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and **not against cash payment**. Further the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's Cheque etc.

66. Quoting of PAN

Permanent account number (PAN) or the equivalent e-documents thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or the equivalent e-documents thereof.

67. Selling Third party products

Bank acting as agent while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

(a) The identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 13(e) of this Policy.

(b) Transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII paragraph 46 of Chapter VII.

(c) AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:

- debit to customers' account or against cheques; and
- obtaining and verifying the PAN given by the account based as well as walk-in customers.

(e) Instruction at (d) above shall also apply to sale of banks' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

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

(a) The 'at par' cheque facility offered by commercial banks to the bank shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.

(b) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC & AML under such arrangements shall be retained by banks. ***(At present the said area is not applicable to us.)***

(c) Bank shall:

i. ensure that the 'at par' cheque facility is utilized only:
   a. for its own use,
   b. for its account-holders who are KYC compliant, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
   c. for walk-in customers against cash for less than rupees fifty thousand per individual.

ii. maintain the following:
   a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,
   b. Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honoring such instruments.

iii. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

69. Issuance of Prepaid Payment Instruments (PPIs): The Bank shall ensure that whenever it starts issuing PPI it will adhere to the instructions issued by Department of Payment and Settlement System of Reserve Bank of India.

70. Hiring of Employees and Employee training:

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

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

(c) On-going employee training program shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues shall be ensured.

71. Deleted from RBI directions

ANNEX I

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 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 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 RE shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) 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.

Banks may use the services of Business Correspondent (BC) for this process.

ANNEX II

File No. 14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division
****

North Block, New Delhi.
Dated: the 2nd February, 2021
(Amended vide corrigendum dated March 15, 2023)
(Amended vide corrigendum dated August 29, 2023)
(Amended vide corrigendum dated April 22, 2024)

ORDER

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

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

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

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

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

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

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

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

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA **[Telephone Number: 011-23093124, 011-230923465 (Fax), email address: jsctcr-mha@gov.in].**

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.4 All the States and UTs shall appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.5 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

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

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

4. Communication of the list of designated individuals/entities:

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

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

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

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

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

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

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

(i) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks, Insurance policies etc., with them.

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

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

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

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

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

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

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

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

6.1 The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction, without delay.

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

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

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

6.5 In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be

issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.

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

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

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

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

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

without delay and inform the UAPA Nodal officer of the State/UT.

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

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

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

v. The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to

sensitize their respective members to the provisions of Section 51A of UAPA, so that if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

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

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

viii. The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms.

Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

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

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

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

8.2 To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by

the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

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

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

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

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

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

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate,

access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

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

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

(a) Interest or other earnings due on those accounts, or

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

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

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

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

11. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person:

11.1 Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.

11.2 The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

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

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

Upon making an application in writing by the concerned individual/organisation, to the concerned bank, stock exchanges/depositories, intermediaries regulated by

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

12. Regarding prevention of entry into or transit through India:

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

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

13. Procedure for communication of compliance of action taken under Section 51A: The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India

was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

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

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

ANNEX III

F.No.P - 12011/2022-ES Cell-DOR

Government of India

Ministry of Finance

Department of Revenue

****

New Delhi, dated the 1st September, 2023.

ORDER

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

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

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

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

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

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

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

iii. derived or generated from the funds or other assets owned or controlled,

directly or indirectly, by such person;

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

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

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

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

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

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

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

implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

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

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') as specified under section 12A (1) to the CNO and Nodal officers.

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

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

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

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

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

3.1 All Financial Institutions shall –

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

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

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

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

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

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned 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/ Commissioners of Police of all States/UTs for initiating suitable action.

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

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

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

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

ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property, and if any match with the designated individuals/entities is found, the Registrar shall immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.

iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of sub- section

(2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post, without delay.

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

4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed, within 24 hours of the verification, if it matches, with the particulars of the designated individual/entity, to the CNO without delay by email, FAX and by post.

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

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

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

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

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

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure that no societies/ firms/ non-profit organizations should be allowed to be registered if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and, in case, such request is received, then the Registrar shall inform the State Nodal Officer, without delay.

(iii) The State Nodal Officer shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial

ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

(iv) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI), requesting them to sensitize their respective members to the provisions of Section 12A, so that, if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

(v) The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(vi) In addition, a member of the ICSI shall, if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical

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

(vii) In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm, and in case such a request is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

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

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

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

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

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

5.3 Further, the State Nodal Officer shall cause to monitor the transactions / accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4. Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such

funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

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

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, consequent to notification by the MEA authorizing access to such funds, assets or resources. This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

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

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

(a) Interest or other earnings due on those accounts, or

(b) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of section 12A of the Act.

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

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

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

(ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and

(iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorize, 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 & the State Nodal Officer.

8. **Procedure for communication of compliance of action taken under Section 12A:** The CNO and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities, frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs, for onward communication to the United Nations.

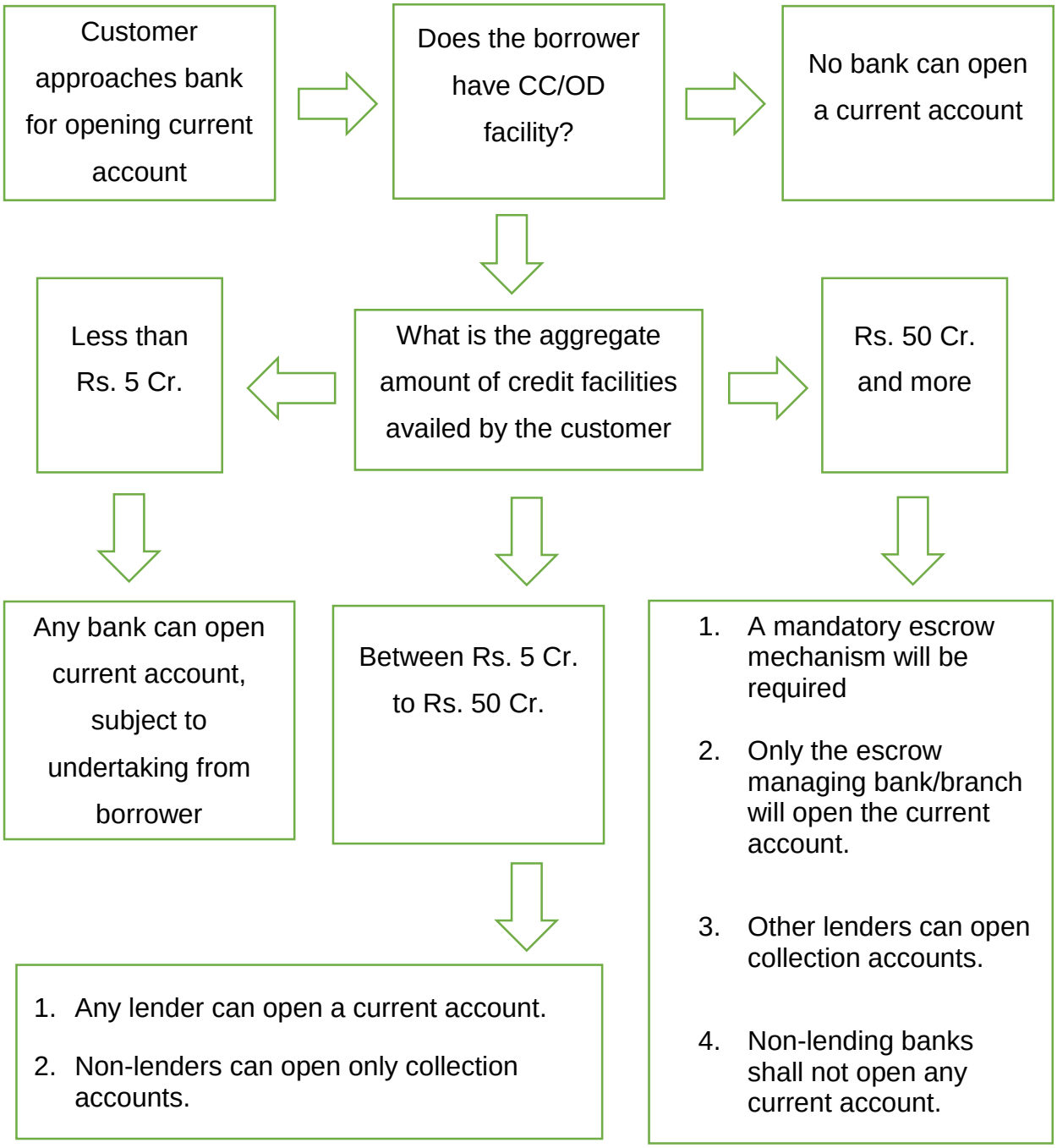
9. **Communication of the Order issued under Section 12A:** The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

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

(Ritvik Ranjanam Pandey)
Joint Secretary to the Government of India

ANNEX IV

FLOW CHART FOR OPENING OF CURRENT ACCOUNT



ANNEX – IV

Examples of STRs received At FIU-IND

Sr. No.	Type of Suspicion	Summary of Detection and Report
1	False Identity	Identification documents found to be forged during customer verification process. The account holder not traceable.
2	Wrong Address	Welcome pack received back since the person was not staying at the given address. In some cases, the address details given by the account holder found to be false. The account holder not traceable.
3	Use of similar sounding corporate names	Account was opened with names very close to other established business entities.
4	Doubt over the real beneficiary of the account	Customer not aware of transactions in the account. Transactions inconsistent with customer's profile.
5	Account of persons under investigation	The customer reported in media for being under investigation/ Account of a customer frozen by the bank
6	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth/Father's name/Nationality) matched with details on a Watch List of UN, Interpol etc.
7	Account used for cyber crime	Complaints of cybercrime received against a customer. The transactions in the account have no valid explanation.
8	Account used for lottery fraud	Complaints received against a bank account used for getting money deposited by victims No valid explanation for the transactions by account holder. Cash withdrawals using ATMs immediately after deposits.
9	Doubtful activity of	Cash deposited in a bank account at multiple cities

	account holder	on the same day. The account holder a citizen of country with high rate of drug trafficking.
10	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
11	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter- account transactions without any economic rationale.
12	Unexplained activity in dormant accounts	The customer could not provide satisfactory explanation to Transactions in a dormant account.
13	Suspicious cash withdrawals in bank account	Large value cheques deposited followed by immediate cash withdrawals.
14	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
15	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list
16	Doubtful utilization of Foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation
17	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization
18	Unexplained activity in Account Inconsistent with what would be expected from declared business	Transactions in account inconsistent with declared business. The Customer could not provide satisfactory explanation.
19	Unexplained large Value	Large value transactions in an account usually

	transactions inconsistent with client's Apparent financial standing	having small Transactions without any economic rationale.
20	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
21	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
22	Doubtful use of safe deposit Locker	Safe deposit locker operated frequently though the financial status of customer does not warrant such frequency. Large suitcase brought by customer.
23	Doubtful source of cash deposited in bank account	Cash transactions of value just under the reporting threshold. Cash transactions spilt across accounts to avoid reporting. No valid explanation

ANNEX – V

SOP FOR ANTI MONEY LAUNDERING (AML) SYSTEM

Chapter I - Preamble

AML software is designed to detect a wide range of activities that may signal money laundering or other financial crimes. By analysing transactional data and customer behaviour, it helps to identify and report suspicious activities to regulatory authorities.

Bank's Anti-money laundering (AML) software generate alerts based on the rules defined by the bank, to detect and prevent activities that may be indicative of money laundering, terrorist financing and/or other financial crimes. These activities can vary widely, but AML software typically focuses on identifying suspicious transactions and behaviours.

Chapter II - Key activities detected under AML software

a) **Unusual Transactions:** AML software is programmed to flag transactions that deviate significantly from a customer's typical behavior or that are unusual for the type of business or industry involved. This could include large cash deposits, rapid movement of funds between accounts, or transactions that seem out of line with a customer's known financial profile.

b) **Structuring:** Structuring involves breaking up large transactions into smaller amounts to avoid triggering reporting requirements. AML software can identify patterns of structuring by monitoring transactions for repetitive, small deposits or withdrawals that may indicate an attempt to evade reporting thresholds.

c) **High-Risk Customers:** AML software helps to identify high-risk customers, such as politically exposed persons (PEPs) or individuals and entities from high-risk jurisdictions. These customers may warrant closer scrutiny due to their potential exposure to corruption, money laundering, or other illicit activities.

d) **Lack of Transparency**: Transactions lacking transparency, such as those involving complex ownership structures or unclear sources of funds, can raise red flags for AML software. The software can analyze transactional data to identify instances

where the true beneficial owners are unnoticeable or where the source of funds is unclear.

e) **Rapid Changes in Account Activity**: Sudden and significant changes in account activity, such as a sharp increase in transaction volume or frequency, can be indicative of illicit behavior. AML software monitors account activity over time to detect such anomalies and alert compliance teams.

f) **Sanctions Violations:** AML software screens transactions against various sanctions lists to identify potential violations. It flags transactions involving individuals, entities, or countries subject to economic sanctions imposed by regulatory authorities.

g) **Peer-to-Peer (P2P) Transactions:** With the rise of digital currencies and peer-to-peer payment platforms, AML software has adapted to monitor these channels for potential money laundering activities. It looks for patterns indicative of illicit fund transfers through peer-to-peer networks.

CHAPTER III - Handling and disposing of AML alerts

The handling and disposing of AML alerts is a critical process for banks to ensure compliance with KYC-AML regulations and to prevent money laundering activities. The procedure for handling and disposing of AML alerts typically involves several key steps, which are as follows:

a) **Alert Generation:** When a potentially suspicious transaction is detected by the bank's monitoring systems, an AML alert is generated. This alert should be reviewed by the branch officials to determine the validity and potential risk associated with the transaction.

b) **Initial Review:** Upon receiving an AML alert, the first step is to conduct an initial review of the alert to assess its validity, relevance and nature of the alert. This may involve gathering additional information related to the alert, such as transaction details, customer profiles, and any other relevant data.

c) **Investigation:** If the AML alert is deemed to be valid and high-risk, a thorough investigation should be initiated. This may involve gathering additional evidence, conducting interviews with relevant parties, and analyzing transactional data to understand the source of funds and the purpose of the transactions.

d) **Risk Assessment:**

i. After the initial review, a risk assessment should be conducted to evaluate the potential risk associated with the alert.
ii. This assessment may consider factors such as the nature of the alert, the customer's profile, transaction patterns, and any other relevant information.
iii. This assessment helps in deciding whether further action is required and what type of action should be taken.

e) **Decision Making:**

i. Based on the findings of the investigation, a decision should be made regarding how to proceed with the AML alert.
ii. This decision may involve disposition of the AML alert as genuine transaction, escalating the alert to Principal Officer (PO) for further review if it seems suspicious or taking appropriate actions based on regulatory requirements and internal policies.

f) **Disposition:**

i. Once a decision has been made regarding the AML alert, appropriate disposition actions should be taken. This may include closing the alert if no further action is required, escalating suspicious transaction for additional review and further reporting by Principal Officer (PO) for filing STR with the relevant authorities.
ii. If in case, no suspicious transaction found in the generated AML alert, branch officials needs to mention the white-listing remark before closing the alert.
iii. Branch officials should dispose-off the AML alerts on daily basis & should ensure that the pendency of alerts shouldn't be more than 7 days from the date of alert generation.

g) **Monitoring and Follow-Up:** After disposing of an AML alert by the branch officials, ongoing monitoring and follow-up is to be undertaken by the Principal Officer to ensure that the actions taken are effective in mitigating money laundering risks. This may involve periodic reviews of closed alerts and reassessment of associated risks.

h) **Reporting & Checking System:**

i. In cases where suspicious activity is identified, branch officials should mark the alert as STR in AML Software and escalate the same to Principal Officer (PO) of the bank for further reporting to FIU-IND.
ii. While reporting such STR, branch officials also need to submit detailed analysis stating the reason for categorizing transaction as suspicious.
iii. After analyzing report submitted by branch, if PO feels that the alert reported by branch doesn't seems suspicious, then PO can whitelist/close that alert at his own, by responding the reason of whitelist/close of said alert to respective branch officials. **OR**

PO will analyze the report submitted by branch & file STR within 7 working days after due diligence of the account and verifying all necessary information required to report FIU-IND. Simultaneously, PO will instruct CPC Department to make change in customer's risk rating in real time as High Risk.

iv. After filing STR, branch should ensure not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no tipping off to the customer at any level.

i) **Record Keeping:** Comprehensive record-keeping is crucial in AML compliance. All documentation, investigations report, decisions, and dispositions related to Suspicious Transaction Report (STR) reported to FIU-IND, should be securely maintained by respective branch and Principal Officer as per regulatory requirements.

Handling and disposing of these alerts require a careful and systematic approach to ensure compliance with regulations and to mitigate the risk of money laundering and terrorist financing.

---------x----------x---------x----------x---------