# FINO Payments Bank Limited

## KYC / AML / CFT Policy

## Version 4.0

## INDEX

## Chapter I: Introduction and applicability

### A. Introduction

1.1. In the recent past, Banking Channels have been misused by miscreants for Money Laundering (ML) and Terrorist Financing (TF) and there have been several such instances domestically and internationally. This has made the role of Banks significant in today's extremely complex economic structure.

1.2. Banks, being highly regulated Entities; have to comply with the Regulator's various guidelines and Directions. Adherences to Know Your Customer (KYC), Anti – Money Laundering (AML), and Countering Financing of Terrorism (CFT) Guidelines are few such requirements that the Banks have to follow for identification and verification of the Customers.

1.3. KYC is to 'Know The Customer's' profile including his occupation/ business activities, address and also the perceived KYC/ AML risk arising out of the relationship. It involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, etc., which in turn helps the banks to manage their risks prudently.

1.4. Money Laundering is

- The illegal process of making large amounts of money generated by a criminal activity, such as drug trafficking, smuggling, human trafficking, etc. appears to have come from a legitimate source.
- The money from the criminal activity is considered dirty, and the process "launders" it to make it look clean
- The 3 stages of money laundering include:
    - i Placement - the illegitimate funds are introduced into the legitimate financial system.
    - ii Layering - the money is moved around to create layers of transactions, sometimes by wiring or transferring through numerous accounts.

iii Integration – in this stage the money is integrated into the financial system through additional transactions until the "dirty money" appears "clean" and assets are created out of it.

**B. Objective**

1.5. This Policy has been framed to develop a strong mechanism for achieving the following objectives:

i To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities.

ii To enable the Bank to know/understand their customers and their financial dealings better, as this in turn helps to manage the associated risks prudently.

iii Establish and verify the identity of the Customers

iv To enable the Bank to comply with all the Legal and Regulatory obligations in respect of KYC / AML / CFT measures / Obligation of Bank under PMLA 2002 and to co-operate with various government bodies dealing with related issues.

**C. Applicability**

1.6. This Policy will be applicable to the following:

i All the Banking activities undertaken by the Bank including Current Account Savings Account (CASA), Domestic Money Transfers, etc., and any other activities that will be undertaken by the Bank in the future based on Regulatory approvals.

ii The Bank also undertakes sale of Third Party Products (TPP) on a non-risk sharing basis and this Policy will be applicable to TPP also.

iii The Branches/ Customer Service Points/ Merchants and any other Channels/ Agents engaged in the Banking activities of the Bank.

iv Employees being onboarded will be subject to KYC and AML requirements as applicable.

**D. Policy Review and Approval**

1.7. This Policy will be reviewed at least annually to incorporate the changes in the KYC/ AML/CFT Guidelines/ Directions, etc.

1.8. The Policy revisions/ amendments will be approved by the Board/ ACB

**E. Roles and Responsibilities**

1.9. The KYC/ AML Team is the author of this Policy and will review this Policy at least once annually to incorporate the changes in the KYC/ AML/CFT Guidelines/ Directions/ Advisories, etc. issued from time to time by RBI/ other Regulators as applicable.

1.10. The Board will review the Policy and approve it

1.11. The First Line of Defense (1st LoD) comprising of Business, Operations, Products, will:

a) Ensure compliance to this Policy and SOPs built around it in the activities carried out by them.

b) The 1st LoD will submit information as required from time to time for KYC/ AML matters to the Compliance/ KYC/ AML Team.

c) Further, the 1st LoD will also cooperate in the various audits including internal audit, RBI audit, Statutory audit, external audits/ reviews and provide information/ data/ MIS as required from time to time.

d) The Product and Process Notes will cover the KYC/ AML areas and the risk mitigants approved through the Product and Process Approval Committee (PAC) Committee.

1.12. The second Line of Defense (2nd LoD) comprises of Compliance Functions including KYC/ AML and Risk Management Teams.

(i) The Compliance Team will:

a) Review the KYC/AML/ CFT Policy and get it approved by Board.

b) W.r.t. KYC/AML/CFT aspects - handle audits including Internal Audit, RBI Audit, Statutory audit, concurrent audit, external audit and close the observations.

c) Submit data/ information to RBI and Financial Intelligence Unit - India (FIU- IND) as required under the Regulatory guidelines and PMLA

d) Review the PAC Notes from KYC/ AML/ CFT perspective and provide feedback.

e) Monitor transactions and submit Suspicious Transaction Report (STR) to FIU-India.

f) Submit various Reports to FIU-India as required under PMLA

(ii) The Risk Management Team will:

a) Conduct RCSA (Risk and Control Self-Assessment) and Monitor the Key Performance Indicators (KPIs) of KYC/ AML areas

b) Review the PAC notes from a Risk perspective

1.13. The third Line of Defense (3rd LoD) is the Internal Audit Department and will carry out audits covering KYC/AML areas in the above two LoDs.

1.14. The Human Resources (HR) Department will ensure that adequate screening mechanism is put in place so that the right types of persons are recruited/ hired as staff.

1.15. Elements of KYC Policy

The KYC Policy consists of the following four key elements:

1) Customer Acceptance Policy

2) Customer Identification Procedures

3) Monitoring of Transactions

4) Risk Management.

1.16. When does KYC apply

KYC will be carried out for the following but is not limited to:

- Opening a new account (deposit)
- When the bank feels it is necessary to obtain additional information from existing customers based on the conduct of the account.
- After periodic intervals based on Guidelines from RBI for periodic updation
- Addition of Joint Holders, signatories, mandate holders, Ultimate Beneficial owners, Power of Attorney holders.
- Change of address
- Change of Customer's profile not limited to customer's occupation/ business activity

## Chapter II: Definitions

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 per cent 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 shareholders agreements or voting agreements.

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

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

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

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% 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. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vi. "Certified Copy" - Obtaining a certified copy by the Bank 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 authorised officer of the RE as per the provisions contained in the Act.

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

• Authorised 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.

vii. "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.

viii. “Customer” means a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

ix. “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner.

x. “Customer identification” means undertaking the process of CDD.

xi. “Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

xii. “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 authorised officer of the RE as per the provisions contained in the Act.

xiii. “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).

xiv. “Domestic and cross-border wire transfer”: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the ‘originator bank’ or ‘beneficiary bank’ is located in different countries such a transaction is cross-border wire transfer.

xv. “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.

xvi. “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.

xvii. "Group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes,
(a) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or
(b) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

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

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

xx. “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

xxi. “Non-face-to-face customer” means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank.

xxii. “Non-profit organization” (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)

xxiii. “Officially Valid Document” (OVD) means the passport, the driving licence, 9proof 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 the 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, post-paid mobile phone, piped gas, water bill);

ii. Property or Municipal tax receipt;

iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government 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 licence 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 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.

xxiv. "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).

xxv. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

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

xxvii. "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).

xxviii. "Politically Exposed Persons" (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials;"

xxix. "Principal Officer" means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Prevention of Money Laundering (maintenance of records) Rules (PMLR).

xxx. "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

xxxi. "Small Account" means a savings account which is opened in terms of sub-rule (5) 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.

xxxii. "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.

xxxiii. "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;

e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f. establishing or creating a legal person or legal arrangement.

xxxiv. "Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the Bank by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the

veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.

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

xxxvi. “Wire transfer” means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

## Chapter III: Customer Acceptance Policy (CAP)

3. As part of the Customer Acceptance Policy, the Bank will verify the identity as laid down in Customer Identification Procedures and the Bank will 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.

   (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) 'Optional'/additional information will be obtained with the explicit consent of the customer after the account is opened.

   (f) The CDD procedure will be applied at the UCIC level.

   (g) If an existing KYC compliant customer of the Bank desires to open another account with another branch, fresh CDD exercise is not required unless there is a change in the demographic details/ profile of the customer. Further, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

   (h) While opening joint accounts, CDD Procedure will be followed for all the joint account holders.

   (i) The Bank will put in place a name screening process 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 (RBI).

   (j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the National Securities Depository Limited (NSDL)/ Income Tax authority/ any other Authority/ facility as made available by the Government of India (GoI).

   (k) Where an equivalent e-document is obtained, the digital signature will be verified as per the provisions of the Information Technology Act, 2000 (21 of 2000).

   (l) It will be ensured that when a customer is permitted to act on behalf of another person/entity, will be clearly spelt out if any circumstances arises.

3.1 It will be ensured that the Customer Acceptance Policy and its implementation does not become too restrictive resulting in denial of banking services to general public, especially to those who are financially or socially at a disadvantage position.

3.2 Pursuant of issuance of guidelines by RBI on “Opening of Current Accounts by Banks - Need for Discipline” dated August 06, 2020 (updated as on December 14, 2020) and consolidated guidelines issued by RBI on April 19, 2022 vide notification on subject “Consolidated Circular on Opening of Current Accounts and CC/OD Accounts by Banks”, guidelines allows any bank can open a current account for customers who either have NIL exposure or the exposure is less than Rupees Five Crore subject to declaration from the customer and necessary check through CIC, CRILC etc. In case of borrowers above Rupees 5 Crore, any one of the lending bank can open a current account and any lending bank can open collection account. Since, our bank cannot have a lending portfolio, only current account will be opened for the customers who will be permitted as per the guidelines. Accordingly, all the customers will be subjected to CIC check at the time of onboarding (other than CRILC). In case the exposure is above Rs. 5.00 Crore, the account opening will not be proceeded and account opening process will be preceded, if the exposure is less than Rs5.00 Crore. As a part of periodic monitoring, all current account customers at the end of May 31 and November 30 of every calendar year will be subject to CIC and CRILC check.

## Chapter IV: Customer Identification Procedure (CIP)

### 4. When Customer identification procedure will be carried out

The Bank shall undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.

(b) Carrying out any international money transfer operations for a person who is not an account holder 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

(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 Rs.50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.

(f) A customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-.

(g) Introduction from an existing customer will not be sought while opening accounts.

### 4.1 Reliance on Third party

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

(a) Records or the information of the CDD carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken to satisfy that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The third party is regulated, supervised, and has measures in place for, compliance with CDD and record-keeping requirements in line with the requirements and obligations under the PMLA.

(d) The third party is not based in a high risk country or jurisdiction.

(e) The Bank will take the ultimate responsibility for CDD and undertaking Enhanced Due Diligence (EDD) measures, as applicable.

## Chapter V: Customer Due Diligence (CDD) Procedure in case of Individuals

### A. Enhanced Due Diligence

**5. Accounts of non-face-to-face customers** (other than Aadhaar OTP based on-boarding): For accounts of non-face-to face customers, the Bank will shall ensure that the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face-to-face customers.

### 5.1. Accounts of Politically Exposed Persons (PEPs)

A. The Bank will establish a relationship with a PEP or where the PEP is a beneficial owner subject to:
(a) Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
(b) The identity of the person has been verified before accepting the PEP as a customer;
(c) The decision to open an account for PEP will be taken at least by a person at Vice President level.
(d) Accounts of PEPs will be subjected to enhanced monitoring
(e) In case an existing customer or the beneficial owner of an existing account subsequently becomes a PEP, approval of at least Vice President level will be obtained to continue the business relationship;
(f) These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

### B. Simplified Due Diligence (SDD)

### 5.2. SDD for Self Help Groups (SHGs)

(a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
(b) CDD of all the office bearers shall suffice.
(c)Customer Due Diligence (CDD) of all the members of SHG will be undertaken at the time of credit linking of SHGs

### 5.3 Account based relationship with an Individual

I. The following information will be obtained from an individual while establishing an account based relationship or while dealing with beneficial owner, authorized signatory or the power of attorney holder related to any legal entities who are individuals:

(a) The Aadhaar number where,
(i) The customer 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) Customer submits his Aadhaar number voluntarily to the Bank
(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; and
(b) The PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 and
(c) Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Bank:
(d) The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation.

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to the bank – the Bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India (UIDAI). 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.
ii) Proof of possession of Aadhaar under clause (aa) above – The Bank will carry out offline verification.
iii) An equivalent e-document of any OVD, the digital signature will be verified 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 will carry out verification through digital KYC as specified under Annex I.

II. 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 RE 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.

III. Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, the Bank will, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner will be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit.

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

Explanation 1: Cases where customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, the Bank will ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

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

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

### 5.4. OTP based e-KYC

Accounts opened using OTP based e-KYC, in non-face-to-face mode, will be subject to the following conditions:

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

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

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

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

v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out.

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

vii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank will clearly indicate that such accounts are opened using OTP based e-KYC and other Banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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

### 5.5 Video based Customer Identification Procedures (V – CIP)

The Bank will undertake live V-CIP, that will be carried out by an official of the Bank, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and will adhere to the following stipulations:

i. The official performing the V-CIP will record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

• Will use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) will be used for aiding the V-CIP.

• 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.

iii. Live location of the customer (Geo-tagging) will be captured to ensure that customer is physically present in India

iv. Ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN to match with the details provided by the customer.

v. Ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

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

vii. All accounts opened through V-CIP will be made operational only after being subject to concurrent audit.

viii. Will ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio - visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. To carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the Bank will carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audio - visual interaction will be initiated from the Bank's domain. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. The video recording will be stored in a safe and secure manner and contain the date and time stamp.

xii. Will ensure to redact or blackout the Aadhaar number.

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

xiv. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly

upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

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

### 5.6 Small Accounts

(i) In case an individual who desires to open a bank account, the Bank will open a 'Small Account', with the following limitations:

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

ii. The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

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

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

(iii) 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 will certify 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 the same 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 will be 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) To 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 of the opening of the said account.

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

(g) Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.
(h) 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 given in Chapter V above.
(i) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Chapter V above.

**5.7 Operation of accounts & money mules:**

(i) “Money Mules” are used by the criminals to launder the proceeds of fraud schemes e.g. phishing and identity theft who gain illegal access to deposit accounts by recruiting third parties to act as ‘Money Mules’. In some cases these third parties may be innocent while in others they may be having complicity with criminals.

(ii) In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment websites, social networking sites, instant messaging and advertisements in newspapers. As and when they are caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times, the address and contact details of such mules are found to be fake or not upto date, making it difficult for enforcement agencies to locate the account holder.

(iii) To ensure to include the names of the money mules reflecting complicity with the criminals in the Internal Watch List and matter will be reported to FIU-India by way of STR. While the accounts of such mule accounts as and when identified, will be closed with the approval of the Incumbent In-charge after giving due notice.

## Chapter VI: CDD Procedure for Sole Proprietary Firms

6.0 For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out as mentioned in Chapter V above.

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

(a) Registration certificate

(b)Certificate/licence issued by Municipal authorities under Shop & Establishment Act.

(c) Sales and income tax returns.

(d) (Provisional/final) CST/VAT/ GST certificate

(e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

(f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(g) 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.

(h) Utility bills such as electricity, water, landline telephone bills, etc.

**6.2.** Cases where the Bank is satisfied that it is not possible to furnish two such documents, the Bank may accept only one of those documents as proof of business/activity along with contact point verification and collection of such other information and clarification as would be required to establish the existence of such firm, and will confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

6.3 The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

## Chapter VII: CDD Procedure for Legal Entities

### 7.0 Identification of Beneficial Owner

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

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

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

### 7.1 Accounts of Companies

For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof will be obtained:
(a) Certificate of incorporation
(b) Memorandum and Articles of Association
(c) Permanent Account Number of the company
(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
(e) Documents, as specified in Chapter V above, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
(f) Certified copies of following documents are also required:
(i) Names of the relevant persons holding senior management position,
(ii) The registered office and the principal place of business, if it different

**(g)** The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

### 7.2 Accounts of Partnership Firms

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:
(a) Registration certificate
(b) Partnership deed
(c) Permanent Account Number of the partnership firm
(d) Documents, as specified in Chapter V above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(e) Certified copies of following documents are also required:
(i) Names of all partners
(ii) Address of the registered office, and the principal place of its business, if it is different.
(f) The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

### 7.3 Accounts of Trust

For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
(a) Registration certificate
(b) Trust deed
(c) Permanent Account Number or Form No.60 of the trust
(d) Documents, as specified in Chapter V above, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
(e) Certified copies of following documents are also required:
(i) The names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and
(ii) List of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust
(f) The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

### 7.4. Accounts of unincorporated association or a body of individuals

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

(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 a body of individuals

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

(d) Relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and Documents, as specified in Chapter V above,

(e) Such information as may be required 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.

(f) The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

### 7.5 Accounts of other Juridical Persons

For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

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

(b) Documents, as specified in Chapter V above, of the person holding an attorney to transact on its behalf and

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

(d) The client shall submit to the Bank any update of any of the documents referred above, for the purpose of updating its records, within 30 days of such updation..

## Chapter VIII - On-going Due Diligence

**8.** The Bank will ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it 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:

(a) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida.

(b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban

**8.1.** Details of accounts resembling any of the individuals/entities in the lists will be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA)

**8.2.** In addition to the above, other UNSCRs circulated by the RBI in respect of any other jurisdictions/ entities from time to time will also be taken note of.

**8.3** To undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

**8.4** High risk accounts will be subjected to more intensified monitoring and the Bank will put in place a mechanism for this purpose.

**8.5.** As mandated by RBI, effective from Sep 2021, the Bank will scrub the entire base of Current Accounts with CRILC & or Credit Information Companies (CICs) and corrective action as deemed fit will be taken for adherence to the guidelines

### 8.5. Periodic Updation

A. Periodic updation will 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 as per the following procedure:

(a) The Bank will shall carry out

i. CDD, as specified in Chapter V above, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect will be obtained.

ii. If there is only address change during periodic updation, a self-certification to that effect will be obtained from customer 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.

iii Accounts of customers, who were minor at the time of opening account, on their becoming major – Bank shall ensure to take fresh photographs and it shall ensure to comply with current CDD standards during periodic updation of customer from minor to major. Bank will ensure to carry out fresh KYC of such customers wherever deemed necessary.

iv. In case of Legal entities, the Bank will review the documents sought at the time of opening of account and obtain fresh certified copies.

v. In case of Legal entities - in case no change in KYC information of LE customer a self-certification to that effect will be obtained. Bank will ensure during the periodic updation process , Beneficial ownership (BO) details available with bank is accurate and up-to date.

vi. Change in KYC information - In case of change in KYC information of LE customer, Bank will undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

Provided, the Bank will ensure that KYC documents, as per extant requirements of the Master Direction, are available.

(b) The Bank will not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., will be acceptable.

(c) The Bank will shall ensure to provide acknowledgment with date of having performed KYC updation.
(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

**B.** In case of existing customers, the Bank will obtain the PAN or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which the Bank will temporarily cease operations in the account till the time the PAN or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank will give the customer an accessible notice and a reasonable opportunity to be heard.
Provided further that if a customer having an existing account-based relationship gives in writing that he does not want to submit his PAN or equivalent e-document thereof or Form No.60, the Bank will close the account and all obligations due in relation to the account will be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

## Chapter IX – Risk Management

### 9. Risk Categorization

(i) Bank will categorize each new customer for the purpose of "Risk" assessment, based on identity, social/financial status, nature of business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. Bank to seek only such information from the customer, which is relevant to the risk category and is not intrusive and will ensure that such information is kept confidential and details/information so collected is not divulged for cross selling or any other purposes.

(ii) For the purpose of risk categorization, individuals (other than High Net Worth clients) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile will be categorized as low risk. [Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location/address of the customer are to be met].

(iii) Categorize customers that are likely to pose a higher than average risk to the bank will be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Bank will apply enhanced due diligence measures based on the risk assessment, requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

(iv) In view of risk involved in cash intensive business, accounts of bullion dealers (including sub-dealers) and jewelers will be categorized as 'high risk' requiring enhanced due diligence.

- Other customers to be categorized as high risk are:
    a. High net worth individuals;
    b. Trusts, charities; NGOs and organizations receiving donations;
    c. Companies having close family shareholding or

d. Politically Exposed Persons [PEPs] ; customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner,
e. Those with dubious reputation as per public information available etc. However, only NPOs/Non – Government Organizations (NGOs) promoted by United Nations or its agencies will be classified as low risk customers.

(v) Bank will periodically review the risk categorization of those accounts which require the need for applying enhanced due diligence measure. Such review of risk categorization of customers should be carried out at a periodicity of not less than once in six months or earlier depending upon the transaction and/or change in status of the account. Bank should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary the source of funds.

(vi) The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by banks are extremely important for effective implementation of KYC/AML/CFT measures. Accordingly, bank will complete the process of risk categorization and compiling/updating profiles of all the existing customers in a time bound manner.

(vii) In addition to what has been indicated above, Bank will take steps to identify and assess the ML/TF risk for customers, countries and geographical areas as also for products / services / transactions / delivery channels and will frame policies, controls and procedures with the approval of the board, to effectively manage and mitigate the risk adopting a risk-based approach as per the initiative taken by IBA.

(viii) Bank will adopt enhanced measures as per the indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring; High & Medium Risk: customers/ Products Services/Geographies/ Locations/ Alerts for branches/ departments that should trigger suspicion at the time of processing of customer’s transaction and not in line with customer’s profile.

## 9.1 Risk Assessment

- The Bank will carry out Risk Assessment exercise to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for customers, countries or geographic areas, products, and delivery channels.
- The assessment process will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.
- The risk assessment will be reviewed annually.
- The outcome of the exercise shall be put up to the Audit Committee of the Board

## Chapter X – Monitoring of Transactions and Reporting to FIU - India

### 10. Principal Officer (PO) – PMLA

- Bank will designate a senior management officer as Principal Officer - PMLA, who will supervise and monitor all the activities in respect of KYC/AML/CFT measures.
- Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. Principal Officer will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.
- The Principal Officer will also be responsible for timely submission of CTRs/STRs/CCRs/NTRs to FIU-India.
- For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data and other Customer Due Diligence information, transaction records and other relevant information.

### 10.1 Designated Director – PMLA

- Bank will designate the Managing Director as the Designated Director – PMLA who will be responsible for the overall implementation of PMLA and Rules thereof in the Bank.

### 10.2 Monitoring of Transactions

(i) On-going monitoring is an essential element of effective KYC procedures. The risk can be effectively controlled and reduced by understanding the normal and reasonable activity of the customer and by having means to identify transactions that fall outside the regular pattern of the activity of the customer. The extent of monitoring will depend on the risk sensitivity of the account. Special attention will paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

(ii) Bank will develop / deploy software for the purpose of monitoring AML alerts based on the pre-defined scenarios. These scenarios will be periodically reviewed to make these more effective based on the feedback received and experience gained.

(iii) Bank will prescribe threshold limits for all categories of accounts on the basis of the nature of business activity, social and financial status, and volume of turnover and location of the customer.

(iv) Monitoring of transactions will broadly involves the following:

- Transactions that involve large amounts of cash inconsistent with customer's normal/expected activity/profile will receive special attention.
- Very high account turnover, inconsistent with the balance maintained, income declared, may indicate the funds are being "washed" through the account.
- Special attention will be paid to all complex, unusually large transactions which have no apparent economic or visible lawful purpose and suspicious patterns that indicate violation of the laws of the country threatening its financial well-being.
- Accounts classified under High Risk will be subjected to more frequent and intensive monitoring based on key indicators taking note of the customers background, country of origin, sources of funds, the type of transactions involved and other risk factors.
- The accounts of bullion dealers (including sub-dealers) and jewelers will be categorized as "High Risk".
- Multi - Level Marketing (MLM) Companies: Transactions in the accounts of MLM will be closely monitored and such accounts will be categorized as "High Risk". Such account will be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.
- Given below is an indicative List of Suspicious Activities Transactions involving large amounts of cash

| **An Indicative List of Suspicious Activities Transactions Involving Large Amounts of Cash** |
|---|
| (i) Exchanging an unusually large amount of small denomination notes for those of higher denomination; |
| (ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank; |
| (iii) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity; |

| |
|---|
| (iv) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad; |
| (v) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.; |
| (vi) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial. |

### 10.3 Reporting to Financial Intelligence Unit-India

- In terms of Prevention Money Laundering Act 2002 and as amended by Prevention Money Laundering (Amendment) Act 2009, Bank will ensure to submit the following reports to Financial Intelligence Unit-India.
- FIU-India has developed a utility i.e. fin NET Project and now Suspicious Transaction Reports (STRs), Counterfeit Currency Reports (CCRs) and Cash Transaction Reports (CTRs) are submitted to them online.

#### 10.3.1 Cash Transaction Report (CTR)

- Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.
- The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

#### 10.3.2. Suspicious Transaction Report (STR)

- While determining suspicious transactions, bank will be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time. Suspicious transaction means a transaction, comprising of deposit, withdrawal, transfer of funds, whether or not made in cash which, to a person acting in good faith:

i. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences laid down under PMLA, 2002, an offence regardless of the value involved; or
ii. appears to be made in circumstances of unusual or unjustified complexity; or
iii. appears to have no economic rationale or bonafide purpose; or
iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism, which includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist act or by a terrorist, terrorist organizations or those who finance or are attempting to financing of terrorism; or

- In some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. Banks will report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

- The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions.

- Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction whether cash or non-cash, series of transactions integrally connected are of suspicious nature.

- Bank will ensure not to put any restrictions on operations in the accounts where Suspicious Transaction Report has been made. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.

### 10.3.3 Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the

transactions will be reported to Financial Intelligence Unit-India in the specified format not later than 15th of the succeeding month from the occurrence of such transactions.

### 10.3.4 Non Profit Organizations Transaction report (NTR)

Bank will report all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013),"

## Chapter XI – General Guidelines

### 11. Secrecy Obligations and Sharing of Information:

(a) The Bank will maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

(b) 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.

(c) While considering the requests for data/information from Government and other agencies, bank will satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

(d) 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.

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

(a) The Bank will capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(d) Capture the KYC information for sharing with the CKYCR as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be, as released by CERSAI from time to time.

(f) To upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR as per the LE Template released by CERSAI.

(g) Once KYC Identifier is generated by CKYCR, the Bank will 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, the Bank will upload/update the KYC data pertaining to accounts of LEs opened prior to 1st April 2021 at the time of periodic updation, or earlier, when the updated KYC information is obtained/ received from the customer.

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

(j) Cases where a customer submits a KYC Identifier for the purposes of establishing an account based relationship, with an explicit consent to download records from CKYCR, then the KYC records would be retrieved online from the CKYCR using the KYC Identifier and the customer will not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

(i) There is a change in the information of the customer as existing in the records of CKYCR;
(ii) The current address of the customer is required to be verified;
(iii) The Bank considers it necessary in order to verify the identity or address of the customer, or to perform EDD or to build an appropriate risk profile of the client.

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

Under FATCA and CRS, the Bank will determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, will take following steps for complying with the reporting requirements:

- Register on the related e-filling portal of Income Tax Department as a Reporting Financial Institutions
- 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: The Bank will 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.
- Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

### 11.3 Period for presenting payment instruments

The Bank will ensure that payment will not be made of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments.

### 11.4. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions will be strictly adhered to, in order to minimise 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." If it is established that an account opened and operated is that of a Money Mule, it will be deemed that the bank has not complied with these directions.

### 11.5. 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.

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

(b) The Bank will not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products but it will be 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.

### 11.7. Introduction of New Technologies – Credit Cards/Debit Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

The Bank will ensure that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies to factor in the money-laundering and financing of terrorism threats that may arise from new or developing technologies.

### 11.8. Correspondent Banks

The Bank will have a Board approved to lay down parameters for approving correspondent banking relationships subject to the following conditions:

(a) Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.

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

(d) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(e) Correspondent relationship shall not be entered into with a shell bank.

(f) It shall be ensured that the correspondent banks do not permit their accounts to be used by shell banks.

(h) To exercise caution while dealing with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(i) To 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.

### 11.9. Wire transfer

The Bank while effecting wire transfer will ensure that:

(a) All cross-border wire transfers including transactions using credit or debit card will be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number.

Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions will be exempt from the above requirements.

(b) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

(c) Customer Identification will be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts will be made to establish his identity and STR shall be made to FIU-IND.
(d) Complete originator information relating to qualifying wire transfers will be preserved at least for a period of five years by the ordering bank.
(e) A bank processing as an intermediary element of a chain of wire transfers will ensure that all originator information accompanying a wire transfer is retained with the transfer.
(f) The receiving intermediary bank will transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.
(g) All the information on the originator of wire transfers will be immediately made available to appropriate law enforcement and/or prosecutorial authorities on receiving such requests.
(h) Effective risk-based procedures to identify wire transfers lacking complete originator information will be in place at a beneficiary bank.
(i) Beneficiary bank will report transaction lacking complete originator information to FIU-IND as a suspicious transaction.
(j) The beneficiary bank will seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary will consider restricting or terminating its business relationship with the ordering bank.

### 11.10. Issue and Payment of Demand Drafts, etc.

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

### 11.11. Selling Third Party Products (TPP)

While selling third party products the Bank will ensure to:

(a) Verify the identity and address of the walk-in customer for transactions above rupees fifty thousand
(b) Transaction details of sale of third party products and related records shall be maintained as detailed in Chapter XII.
(c) These TPP transactions will be monitored for the purpose of filing CTR/STR including walk-in customers.
(d) Transactions involving rupees fifty thousand and above for sale of Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product will 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.

**11.12. Issuance of Prepaid Payment Instruments (PPIs):**

The Bank while issuing PPIs will ensure that the instructions issued by Department of Payment and Settlement System (RBI) through their Master Direction are strictly adhered to.

**11.13 Freezing of Assets u/s 51A of Unlawful Activities (Prevention) Act, 1967**

The procedure laid down in the UAPA Order dated February 2, 2021 (Annexure II) 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 Home Affairs.

**11.14 Jurisdictions that do not or insufficiently apply the FATF Recommendations**

(a) Financial Action Task Force (FATF) Statements circulated by RBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, will be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement will be taken into account.
(b) Special attention will 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.

(c) 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 will be examined, and written findings together with all documents will be retained and shall be made available to RBI/ other relevant authorities, on request.

**11.15 Registering of NPO (Non-profit Organization) on the DARPAN Portal**

The Bank shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the Bank has ended or the account has been closed, whichever is later..

## Chapter XII – Maintenance and Preservation of Records

12. For reporting of customer account information, with reference to provisions of PML Act and Rules, the Bank will:

(a) 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;

(b) 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;

(c) Make available the identification records and transaction data to the competent authorities upon request;

(d) Maintain all necessary information in respect of transactions prescribed under Prevention of Money Laundering (Maintenance of Records) Rules, 2005 Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) Nature of the transactions;

(ii) Amount of the transaction and the currency in which it was denominated;

(iii) Date on which the transaction was conducted; and

(iv) Parties to the transaction.

(e) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005) in hard or soft format.

(f) Registering of NPO (Non-profit Organization) on the DARPAN Portal

Bank should have an infrastructure or system in place to maintain registration records of NPO (Non-profit Organization) who have been registered on the DARPAN portal of NITI Aayog, for period of 5 years after the business relationship between the client and RE (Reporting entity) has ended or account has been closed, whichever is later.

## Chapter XIII - Hiring of Employees and Employee training

13.1 Adequate screening mechanism as an integral part of their personnel recruitment/hiring process will be put in place.

13.2 On-going employee training programme will be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training will be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff will 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.

### 13.3 Training of Employees

The Bank will ensure to have ongoing employee training programmes/seminar in order to sensitize the field staff about KYC/AML/CFT procedures/ modalities/guidelines and changes from time to time. AML Department of the Bank will put in place an appropriate training content and channelize the same in association with Training team and HR department.

***Annexure I***

## Digital KYC Process

A. The Bank will 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 will be controlled by the Bank and it will 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, will 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 will 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 will 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 will 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 will 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), will be captured vertically from above and water-marking in readable form as mentioned above will 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 will 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 will 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 RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the Bank will 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 will 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. The Bank may use the services of Business Correspondent (BC) for this process.

***Annexure II***

**UAPA Order dated 2nd February 2021**

File No. 14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division
North Block, New Delhi.
Dated: 2nd February, 2021

**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: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].**

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

3.4 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.

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;

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

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

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

11.3 The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of

State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.

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

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

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

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

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

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

## GLOSSARY

| | |
|---|---|
| AML | Anti – Money Laundering |
| BO | Beneficial Owner |
| CASA | Current Account Savings Account |
| CBDT | Central Board of Direct Taxes |
| CBS | Core Banking Solution |
| CCR | Counterfeit Currency Reports |
| CDD | Customer Due Diligence |
| CERSAI | Central Registry of Securitisation Asset Reconstruction and Security Interest of India |
| CFT | Countering Financing of Terrorism |
| CIP | Customer identification procedure |
| CKYCR | Central KYC Records Registry |
| CRS | Common Reporting Standards |
| CTRs | Cash Transaction Reports |
| EDD | Enhanced Due Diligence |
| FATCA | Foreign Account Tax Compliance Act |
| FATF | Financial Action Task Force |
| FEDAI | Foreign Exchange Dealers' Association of India |
| FIU- IND | Financial Intelligence Unit – India |
| GoI | Government of India |
| IGA | Inter - Governmental Agreement |
| KPI | Key Performance Indicators |
| LEs | Legal Entities |
| LoD | Line of Defence |
| MHA | Ministry of Home Affairs |
| ML | Money Laundering |
| MLM | Multi - Level Marketing |
| NGOs | Non – Government Organizations |
| NPO | Non-profit organisations |
| NRIs | Non-Resident Indians |
| NTR | Non Profit Organizations Transaction Report |

| | |
|---|---|
| OVD | Officially Valid Document |
| PAC | Product and Process Approval Committee |
| PAN | Permanent Account Number |
| PEP | Politically Exposed Person |
| PIOs | Persons of Indian Origin |
| PMLA | Prevention of Money Laundering Act |
| PMLR | Prevention of Money Laundering (Maintenance of Records) Rules |
| PO | Principal Officer |
| PPIs | Prepaid Payment Instruments |
| RCSA | Risk and Control Self-Assessment |
| SDD | Simplified Due Diligence |
| SHG | Self Help Group |
| STR | Suspicious Transaction Report |
| TF | Terrorist Financing |
| TPP | Third Party Products |
| UAPA | Unlawful Activities (Prevention) Act |
| UCIC | Unique Customer Identification Code |
| UIDAI | Unique Identification Authority of India |
| UNSC | United Nations Security Council |
| V-CIP | Video based Customer Identification Process |