

**Draft Reserve Bank of India (Small Finance Banks – Know Your Customer)  
Directions, 2025**

**DRAFT FOR COMMENTS**

**RBI/2025-26--  
DoR.AML.REC.No./00-00-000/2025-26**

**XX, 2025**

**Reserve Bank of India (Small Finance Banks – Know Your Customer) Directions,  
2025**

**Table of Contents**

|  |           |
|--|-----------|
| <b>CHAPTER I - PRELIMINARY.....</b>  | <b>4</b>  |
| <b>CHAPTER II - General .....</b>  | <b>15</b> |
| <b>CHAPTER III - Customer Acceptance Policy.....</b>   | <b>18</b> |
| <b>CHAPTER IV - Risk Management.....</b>   | <b>20</b> |
| <b>Chapter V - Customer Identification Procedure (CIP).....</b>  | <b>21</b> |
| <b>Chapter VI - Customer Due Diligence (CDD) Procedure .....</b>   | <b>23</b> |
| <b>Chapter VII - Record Management .....</b>   | <b>48</b> |
| <b>Chapter VIII - Reporting Requirements to Financial Intelligence Unit – India.....</b>   | <b>50</b> |
| <b>Chapter IX - Requirements/obligations under International Agreements -<br/>Communications from International Agencies .....</b> | <b>52</b> |
| <b>Chapter X - Other Instructions .....</b>  | <b>56</b> |
| <b>Chapter XI - Repeal and Other Provisions .....</b>  | <b>68</b> |
| <b>Annex I .....</b>   | <b>69</b> |
| <b>Annex II .....</b>  | <b>84</b> |

## **Introduction**

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF), which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, as a member of FATF, is committed to upholding measures to protect the integrity of the international financial system.

In India, the Prevention of Money-Laundering Act, 2002, and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). The provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, require Regulated Entities (REs) to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise, and to monitor their transactions.

Accordingly, in exercise of the powers conferred by sections 35A of the Banking Regulation Act, 1949, section 10(2) read with section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and all other laws enabling the Reserve Bank in this regard, the RBI being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

## CHAPTER I - PRELIMINARY

### **A. Short Title and Commencement.**

1. These Directions shall be called the Reserve Bank of India (Small Finance Bank – Know Your Customer) Directions, 2025.
2. These Directions shall come into effect on the day the RBI places them on its official website.

### **B. Applicability**

3. These Directions shall be applicable to Small Finance Banks (hereinafter collectively referred to as 'banks' and individually as a 'bank').
4. These directions shall also apply to those branches and majority-owned subsidiaries of the bank which are located abroad, to the extent they are not contradictory to the local laws in the host country, provided that:
  - (1) where applicable laws and regulations prohibit implementation of these guidelines, the bank shall bring the same to the notice of the RBI. The RBI may advise the bank to take further necessary action, including application of additional measures to manage the ML / TF risks.
  - (2) in case there is a variance in KYC / AML standards prescribed by the RBI and the host country regulators, branches / subsidiaries of the bank shall adopt the more stringent regulation of the two.

**Provided that** this rule shall not apply to 'small accounts' referred to in paragraph 28 of Chapter VI.

### **C. Definitions**

5. In these Directions, unless the context otherwise requires, the following meanings are assigned to the terms herein:
  - (1) Terms bearing meaning assigned in terms of the Prevention of Money-Laundering Act, 2002, and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:
    - (i) 'Aadhaar number' shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
    - (ii) 'Act' and 'Rules' mean 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 exercises control through other means.

***Explanation:*** For the purpose of this sub-clause-

- ‘Controlling ownership interest’ means ownership of / entitlement to more than 10 percent of the shares or capital or profits of the company.
  - ‘Control’ shall include the right to appoint the 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(s), has / have ownership of / entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

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

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

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

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

- (v) ‘Certified Copy’ – obtaining the 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 the officially valid document produced by the customer with the original, and an authorised officer of the bank shall record the comparison on the copy 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)}, the bank may alternatively obtain the original certified copy, certified by any one of the following:
- (a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
  - (b) branches of overseas banks with whom Indian banks have relationships,
  - (c) Notary Public abroad,
  - (d) Court Magistrate,
  - (e) Judge,
  - (f) Indian Embassy / Consulate General in the country where the non-resident customer resides.
- (vi) ‘Central KYC Records Registry’ (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- (vii) ‘Designated Director’ means a person whom the bank designates to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, whom the Board of Directors has duly authorised.
- Explanation:*** For the purpose of this clause, the terms ‘Managing Director’ and ‘Whole-time Director’ shall have the meaning assigned to them in the Companies Act, 2013.
- (viii) ‘Digital KYC’ means that an authorised officer of the bank captures a 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, as per the provisions contained in the Act.
- (ix) ‘Digital Signature’ shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- (x) ‘Equivalent e-document’ means an electronic equivalent of a document that the

issuing authority of such document issues with its valid digital signature, including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

- (xi) 'Group' – The term 'group' shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).
- (xii) 'Know Your Client (KYC) Identifier' means the unique number or code that the Central KYC Records Registry assigns to a customer.

**Explanation:** A customer can obtain his KYC Identifier through the following ways:

In the process of opening an account, once the customer's KYC Identifier is generated by CKYCR and provided to the bank, the latter shall share the same with the concerned customer. The customer can also access his KYC Identifier on CKYCR Portal ([www.ckycindia.in](http://www.ckycindia.in)).

- (xiii) 'Non-profit organisations' (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 or any similar State legislation or a company registered under section 8 of the Companies Act, 2013 (18 of 2013).
- (xiv) 'Officially Valid Document' (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card that the Election Commission of India issues, the job card that NREGA issues and an officer of the State Government duly signs, and the letter that the National Population Register issues 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 that the Unique Identification Authority of India (UIDAI) issues.
- (b) When the customer furnishes an OVD that does not have an updated address, the bank shall deem the following documents or the equivalent e-documents thereof to be OVDs for the limited purpose of proof of address:-
  - utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
  - property or Municipal tax receipt;

- pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- letter of allotment of accommodation from employer that is 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;

**Illustration:** If a customer is staying in Chennai but their OVD contains an address of New Delhi, they can open an account in Chennai by submitting a *deemed to be* OVD for the purpose of proof of address. However, as mentioned below in clause (c), they are required to submit an OVD with current address within a period of three months.

- (c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at (b) above
- (d) if the OVD that a foreign national presents does not contain the details of address, the bank shall accept documents that Government departments of foreign jurisdictions issue, and a letter that the Foreign Embassy or Mission in India issues, as proof of address.

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

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

(xvi) 'Person' has the same meaning assigned in the Act and includes:

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

persons (a to f).

(xvii) ‘Principal Officer’ means a bank’s nominated officer at the management level, responsible for furnishing information as per rule 8 of the Rules.

(xviii) ‘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 have no 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 that the bank suspects are linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

(xix) A ‘Small Account’ means a savings account which is opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in paragraph 28.

(xx) ‘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.

(2) Unless the context otherwise requires, terms in these Directions shall bear the meanings assigned to them below:

(i) ‘Common Reporting Standards’ (CRS) means reporting standards set for

implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

- (ii) Correspondent Banking: Correspondent banking is the provision of banking services by one bank (the ‘correspondent bank’) to another bank (the ‘respondent bank’). A correspondent bank may provide the respondent banks with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
- (iii) ‘Customer’ means a person who is engaged in a financial transaction or activity with the bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- (iv) ‘Walk-in Customer’ means a person who does not have an account-based relationship with the bank, but undertakes transactions with the bank.
- (v) ‘Customer Due Diligence (CDD)’ means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

***Explanation:*** The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding ₹ 50 thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

- (a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable
- (b) Taking reasonable steps to understand the nature of the customer’s business, and its ownership and control;
- (c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.
- (vi) ‘Customer identification’ means undertaking the process of CDD.
- (vii) ‘FATCA’ means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

- (viii) 'IGA' means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
- (ix) 'KYC Templates' means templates prepared to facilitate collating and reporting KYC data to the CKYCR, for individuals and legal entities.
- (x) 'Non-face-to-face customers' means customers who open accounts without visiting the branch / offices of the bank or meeting the officials of the bank.
- (xi) 'On-going Due Diligence' means regular monitoring of transactions in accounts to ensure that transactions are consistent with the bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
- (xii) Payable-through accounts: The term payable-through accounts refers to correspondent accounts that third parties use directly to transact business on their own behalf.
- (xiii) 'Periodic Updation' means the steps taken to ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the RBI.
- (xiv) 'Regulated Entities' (REs) means:
  - (a) all Scheduled Commercial Banks (SCBs) / Regional Rural Banks (RRBs) / Local Area Banks (LABs) / All Primary (Urban) Co-operative Banks (UCBs) / State and Central Co-operative Banks (StCBs / CCBs), and any other entity which has been licensed under section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'
  - (b) All India Financial Institutions (AIFIs)
  - (c) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
  - (d) Asset Reconstruction Companies (ARCs)
  - (e) All Payment System Providers (PSPs) / System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
  - (f) All authorised persons (APs), including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
- (xv) 'Shell Bank' means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute

physical presence.

- (xvi) 'Video based Customer Identification Process (V-CIP)': an alternative method by which an authorised official of the bank conducts customer identification with facial recognition and customer due diligence. This process involves a seamless, secure, live, informed- consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information which the customer furnished, through independent verification and by maintaining an audit trail of the process. The bank shall treat such processes complying with prescribed standards and procedures on par with face-to-face CIP for the purpose of this Direction.
- (xvii) 'Wire transfer' related definitions:
- (a) Batch transfer: A batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may / may not be ultimately intended for different persons.
  - (b) Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement whom / which the originator identifies as the receiver of the requested wire transfer.
  - (c) Beneficiary RE: It refers to a financial institution that RBI regulates, which receives the wire transfer from the ordering financial institution directly or through an intermediary RE and makes the funds available to the beneficiary.
  - (d) Cover Payment: Cover Payment refers to a wire transfer that combines a payment message which the ordering financial institution sends directly to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
  - (e) Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
  - (f) Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfers that takes place entirely within the borders of India, even though

- the system used to transfer the payment message may be located in another country.
- (g) Financial Institution: In the context of wire-transfer instructions, the term ‘Financial Institution’ shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
  - (h) Intermediary RE: Intermediary RE refers to an RBI regulated financial institution / entity that handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
  - (i) Ordering RE: Ordering RE refers to the RBI-regulated financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
  - (j) Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
  - (k) Serial Payment: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).
  - (l) Straight-through Processing: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.
  - (m) Unique transaction reference number: Unique transaction reference number refers to a combination of letters, numbers or symbols, a payment service provider determines, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
  - (n) Wire transfer: Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

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

## **CHAPTER II - General**

### **A. Board of Directors / Policies related guidelines:**

#### **6. Know Your Customer (KYC) Policy:**

- (1) The bank shall have a KYC policy. The Board of Directors of the bank, or any committee to which the power has been delegated, shall duly approve the KYC policy.
- (2) The KYC policy shall include following four key elements:
  - (i) Customer Acceptance Policy;
  - (ii) Risk Management;
  - (iii) Customer Identification Procedures (CIP); and
  - (iv) Monitoring of Transactions
- (3) The KYC policy shall, inter alia, incorporate provisions for the following:
  - (i) Periodic updation of KYC
  - (ii) Any exceptional measures for KYC updation, such as requiring a recent photograph, physical presence, or a more frequent updation schedule than the minimum prescribed.
  - (iii) Obtaining a copy of OVD or deemed OVD, for the purpose of proof of change of address during KYC updation.
  - (iv) Providing facility of updation / periodic updation of KYC at any branch.
  - (v) Furthermore, the bank shall have the following:
    - (a) Policies approved by the Board detailing a robust due diligence process for managing requests to change the registered Mobile Number for Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode.
    - (b) Policy approved by the Board or a committee headed by the Chairman / CEO / MD, to establish parameters for approving cross-border correspondent banking relationships. New correspondent banking relationships require post facto approval from the Board or the empowered committee.

(15 of 2003). Accordingly, every bank which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence, money laundering, and terrorist finance risk management, and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

9. Bank's policy framework shall seek to ensure compliance with PML Act / Rules, including regulatory instructions in this regard and shall provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance with the legal / regulatory requirements as above, the bank may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.
10. Money Laundering and Terrorist Financing Risk Assessment by the bank:
  - (1) The bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercises periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator / supervisor may share with the bank from time to time.
  - (2) The bank shall properly document its risk assessment and it shall be proportionate to the nature, size, geographical presence, complexity of activities / structure, etc. of the bank. Further, the Board or a committee of the Board to which it has delegated power shall determine the periodicity of the risk assessment exercise, in alignment with the outcome of the risk assessment exercise. However, the bank shall review it at least annually.
  - (3) The bank shall present the outcome of the exercise to the Board or any committee of the Board to which power in this regard has been delegated, and the outcome shall also be made available to competent authorities and self-regulating bodies.
11. The bank shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on its own or through national risk assessment) and shall

have Board-approved policies, controls and procedures in this regard. The bank shall implement a CDD programme, having regard to the ML / TF risks identified and the size of business. Further, the bank shall monitor the implementation of the controls and enhance them if necessary.

12. Compliance of KYC policy: The bank shall ensure compliance with KYC Policy through:
  - (1) specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
  - (2) allocation of responsibility for effective implementation of policies and procedures.
  - (3) independent evaluation of the compliance functions of the bank's policies and procedures, including legal and regulatory requirements.
  - (4) concurrent / internal audit system to verify compliance with KYC / AML policies and procedures.
  - (5) submission of quarterly audit notes and compliance to the Audit Committee.
13. The bank shall ensure that it does not outsource the decision-making functions of determining compliance with KYC norms.

## **B. Other General Guidelines:**

14. Designated Director:
  - (1) A 'Designated Director' is a Board-nominated person whom the bank designates to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
  - (2) The bank shall communicate the name, designation, address, and contact details of the Designated Director to the FIU-IND and RBI.
  - (3) The bank shall not nominate the Principal Officer as the 'Designated Director'.
15. Principal Officer:
  - (1) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law / regulations.
  - (2) The bank shall communicate the name, designation, address, and contact details of the Principal Officer to the FIU-IND and RBI.

### **CHAPTER III - Customer Acceptance Policy**

16. The bank shall frame a Customer Acceptance Policy.
17. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, the bank shall:
  - (1) not to open any account in an anonymous or fictitious / benami name.
  - (2) open no account where it is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or unreliability of the documents / information furnished by the customer. The bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
  - (3) not undertake a transaction or commence an account-based relationship without following the CDD procedure.
  - (4) specify the mandatory information to be sought for KYC purposes while opening an account and during the periodic updation.
  - (5) obtain additional information, where its internal KYC Policy has not specified such information requirement, with the explicit consent of the customer.
  - (6) apply the CDD procedure at the UCIC level. Thus, if an existing KYC-compliant customer of a bank desires to open another account or avail of any other product or service from the same bank, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned.
  - (7) follow the CDD Procedure for all the joint account holders, while opening a joint account.
  - (8) clearly spell out the circumstances in which a customer is permitted to act on behalf of another person / entity.
  - (9) put in place a suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of these Directions.
  - (10) verify the Permanent Account Number (PAN) (if obtained) from the verification facility of the issuing authority.
  - (11) verify the customer's digital signature on the equivalent e-document (if obtained) as per the provisions of the Information Technology Act, 2000 (21 of 2000).
  - (12) verify the Goods and Services Tax (GST) number from the search / verification facility of the issuing authority, where the GST details are available.
18. The Customer Acceptance Policy shall not result in denial of a banking / financial

facility to members of the general public, especially those who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). The bank shall not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned shall duly record the reason(s) for rejection.

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

## **CHAPTER IV - Risk Management**

20. For risk management, the bank shall have a risk-based approach which includes the following.
  - (1) The bank shall categorise customers into low, medium, and high-risk categories, based on its assessment and risk perception.
  - (2) The bank may lay down broad principles for the risk-categorisation of customers.
  - (3) The bank shall undertake risk categorisation based on parameters such as the customer's identity, social / financial status, nature of business activity, and information about the customer's business and its location, geographical risk covering customers as well as transactions, type of products / services offered, delivery channel used for delivery of products / services, types of transactions undertaken such as cash, cheque / monetary instruments, wire transfers, forex transactions, etc. The bank may also factor in the ability to confirm identity documents through online or other services offered by issuing authorities, while considering customer's identity.
  - (4) The bank shall keep the risk categorisation of a customer and the specific reasons for such categorisation confidential and shall not reveal this information to the customer to avoid tipping off.

***Provided that*** the bank collects various other non-intrusive information from different categories of customers relating to the perceived risk, and specifies the same in the KYC policy.

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

## **Chapter V - Customer Identification Procedure (CIP)**

21. The bank shall undertake identification of customers in the following cases:
  - (1) Commencement of an account-based relationship with the customer.
  - (2) Carrying out any international money transfer operations for a person who is not an account holder of the bank.
  - (3) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
  - (4) Selling third-party products as agents, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than ₹50 thousand.
  - (5) Carrying out transactions for a non-account-based customer, i.e., a walk-in customer, where the amount involved is equal to or exceeds ₹50 thousand, whether conducted as a single transaction or several transactions that appear to be connected.
  - (6) When the bank has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of ₹50 thousand.
  - (7) The bank shall ensure it does not seek introductions while opening accounts.
22. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship or while carrying out an occasional transaction of an amount equal to or exceeding ₹50 thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, the bank, shall at its option, rely on customer due diligence done by a third party, subject to the following conditions:
  - (1) The bank obtains the records or information of the customer due diligence carried out by the third party immediately from the third party or from the Central KYC Records Registry.
  - (2) The bank shall take adequate steps to satisfy itself that the third party will make copies of identification data and other relevant documentation relating to the customer due diligence requirements available, upon request, without delay.
  - (3) A regulator regulates, supervises, or monitors the third party, and the third party has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
  - (4) The bank shall ensure that the third party is not based in a country or jurisdiction assessed as high-risk.

- (5) The bank will have the ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable.

## **Chapter VI - Customer Due Diligence (CDD) Procedure**

### **A. Customer Due Diligence (CDD) Procedure in case of Individuals**

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

- (1) the Aadhaar number where,
  - (i) they are 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) they decide to submit their Aadhaar number voluntarily to a bank or any RE notified under the first proviso to sub-section (1) of section 11A of the PML Act; or
- (2) the proof of possession of Aadhaar number where the bank can carry out offline verification; or
- (3) the proof of possession of Aadhaar number where the bank cannot carry out the offline verification or any OVD or the equivalent e-document thereof containing the details of their identity and address; or
- (4) the KYC Identifier with an explicit consent to download records from CKYCR; and
- (5) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
- (6) the bank may require such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof.

***Provided that*** where the customer has submitted,

- (i) Aadhaar number under clause (1) above to a bank or to a RE notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank shall carry out authentication of the customer's Aadhaar number using UIDAI's e-KYC authentication. Further, in such a case, if the customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, they may give a self-declaration to that effect to the bank.

- (ii) proof of possession of Aadhaar under clause 25(2) above where offline verification can be carried out, the bank shall carry out offline verification.
- (iii) an equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take a live photo as specified under paragraph 24 below.
- (iv) any OVD or proof of possession of Aadhaar number under clause (3) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC as specified under paragraph 24 below.
- v) KYC Identifier under clause (4) above, the bank shall retrieve the KYC records online from the CKYCR in accordance with paragraph 65.

**Provided that** for a period not beyond such date as the Government may notify for a class of REs, instead of carrying out digital KYC, the bank pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where the customer does not submit an equivalent e-document.

**Provided further that** in case the bank cannot perform an e-KYC authentication 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 shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. An official of the bank shall invariably carry out CDD done in this manner, and such exception handling shall also be a part of the concurrent audit as mandated in paragraphs 12 and 13. 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. The bank shall subject the database to periodic internal audit / inspection and the bank shall make database available for supervisory review.

**Explanation 1:** The bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the

authentication of Aadhaar number is not required as per proviso (i) above.

**Explanation 2:** A bank official, business correspondent, or business facilitator can perform biometric-based e-KYC authentication, including Aadhaar Face Authentication.

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

**Explanation 4:** Aadhaar number is not mandatory for purposes of KYC. However, in case 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), the customer shall provide the Aadhaar number to the bank. In other cases, customers may provide the Aadhaar number voluntarily.

24. Digital KYC Process:

- (1) The bank shall develop an application for digital KYC process and make it available at customer touch points for undertaking KYC of its customers and shall undertake the KYC process only through this authenticated application.
- (2) The bank shall control the access to the Application and shall ensure that unauthorised persons do not use it. Authorised officials shall access the Application only through a login-id and password or a Live OTP or Time OTP controlled mechanism that the bank provides.
- (3) The customer, for the purpose of KYC, shall visit the location of the authorised official of the bank or vice-versa. The original OVD shall be in possession of the customer.
- (4) The bank shall ensure that the authorised officer takes a Live photograph of the customer and embeds the same photograph in the Customer Application Form (CAF). Further, the bank's system Application shall put a watermark in readable form, containing the CAF number, GPS coordinates, authorised official's name, unique employee code (which the bank assigns) and date (DD:MM:YYYY) and time stamp (HH:MM:SS), on the captured live photograph of the customer.
- (5) The bank's Application shall have the feature that it captures only a live photograph of the customer and does not capture any printed or video graphed photograph. The background behind the customer while capturing live photograph shall be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

- (6) Similarly, the authorised officer shall capture the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), vertically from above and shall apply a water-marking in readable form as mentioned above. The authorised officer shall ensure there is no skew or tilt in the mobile device while capturing the live photograph of the original documents.
- (7) The authorised officer shall capture the live photograph of the customer and his original documents in proper light so that they are clearly readable and identifiable.
- (8) Thereafter, the authorised officer shall fill all the entries in the CAF as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details may 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 may be auto-populated by scanning the QR available on Aadhaar / e-Aadhaar.
- (9) 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, the bank will treat it as the customer's signature on CAF. However, if the customer does not have their own mobile number, the bank may use the mobile number of their family / relatives / known persons for this purpose and clearly mention it in the CAF. In any case, the bank shall not use the mobile number of authorised officer registered with the bank for the customer signature. The bank shall check that the mobile number used in customer signature is not the mobile number of the authorised officer.
- (10) The authorised officer shall provide a declaration about the capturing of the live photograph of the customer and original document. For this purpose, the bank shall verify the authorised officer with One Time Password (OTP) which will be sent to his mobile number registered with the bank. Upon successful OTP validation, the bank shall treat it as the authorised officer's signature on the declaration. The live photograph of the authorised officer shall also be captured in this authorised officer's declaration.
- (11) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the bank, and also generate the transaction-id / reference-id number of the process. The authorised officer shall intimate the details regarding transaction-id / reference-id number to the customer for future reference.

- (12) The authorised officer of the bank shall check and verify that:
- (i) information available in the picture of the document matches with the information entered by authorised officer in CAF.
  - (ii) live photograph of the customer matches with the photo available in the document.; and
  - (iii) the authorised officer has properly filled all of the necessary details in CAF, including mandatory field.
- (13) On Successful verification, the CAF shall be digitally signed by authorised 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.
- (14) The bank may use the services of Business Correspondent (BC) for this process.
25. Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:
- (1) The Customer shall give specific consent for the authentication through OTP.
  - (2) As a risk-mitigating measure for such accounts, the bank shall ensure that it sends transaction alerts, OTP, etc., only to the mobile number of the customer registered with Aadhaar. The bank shall have a Board-approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
  - (3) The aggregate balance of all the deposit accounts of the customer shall not exceed ₹one lakh. In case the balance exceeds the threshold, the bank shall cease the account's operation, until it completes the CDD as mentioned at (06) below.
  - (4) The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed ₹two lakh.
  - (5) As regards borrowing accounts, the bank shall sanction only term loans. The aggregate amount of term loans sanctioned shall not exceed ₹60 thousand in a year.
  - (6) The bank shall not allow accounts, both deposit and borrowing, opened using OTP based e-KYC to operate for more than one year unless it carries out identification as per paragraph 23 or as per paragraphs 26 and 27 (V-CIP). If the bank uses Aadhaar details under paragraphs 26 and 27 it shall follow the process in its entirety, including fresh Aadhaar OTP authentication.
  - (7) If the bank does not complete the CDD procedure as mentioned above within a year; (a) in respect of deposit accounts, the bank shall close the same immediately, and (b) in respect of borrowing accounts, the bank shall allow no further debits.

- (8) The bank shall obtain declaration 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 RE. Further, while uploading KYC information to CKYCR, bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face- to-face mode.
  - (9) The bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance / violation, to ensure compliance with the above-mentioned conditions.
26. The bank may undertake V-CIP to carry out:
- (1) CDD in case of new customer onboarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.  
*Provided that* in case of CDD of a proprietorship firm, the bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in paragraph 31 and paragraph 32, apart from undertaking CDD of the proprietor.
  - (2) Conversion of existing accounts opened in non-face-to-face mode using Aadhaar OTP based e-KYC authentication as per paragraph 25.
  - (3) Updation / Periodic updation of KYC for eligible customers.

27. The bank opting to undertake V-CIP, shall adhere to the following minimum standards:
- (1) V-CIP Infrastructure
    - (i) The bank shall have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The bank shall house the technology infrastructure in its own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall comply with relevant RBI guidelines. Where the bank uses a cloud deployment model, it shall ensure that ownership of data in such model rests with the bank only and all the data including video recording is transferred to the bank's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and the cloud service provider or third-party technology provider assisting the V-CIP shall retain no data.

- (ii) The bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The bank shall record the customer consent in an auditable and alteration-proof manner.
- (iii) The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- (iv) The video recordings shall contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date and time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
- (v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the bank.

***Explanation:*** Making specific facial gestures, like blinking of eyes, smiling, frowning, etc. is not mandatory for liveness check. The bank shall take due cognizance of special needs, if any, of the customer during liveness check.

- (vi) The bank may use appropriate artificial intelligence (AI) technology to ensure that the V-CIP is robust.
- (vii) Based on experience of detected / attempted / ‘near-miss’ cases of forged identity, the bank shall regularly update the technology infrastructure including application software as well as workflows. The bank shall report any detected case of forged identity through V-CIP as a cyber event under extant regulatory guidelines.
- (viii) The bank shall subject the V-CIP infrastructure to necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. The bank shall mitigate any critical gap reported under this process before rolling out its implementation. The empaneled auditors of Indian Computer Emergency Response Team (CERT-In) shall conduct such tests. Such tests shall also be carried out periodically in conformance to internal / regulatory guidelines.
- (ix) The bank shall subject the V-CIP application software and relevant APIs / webservices to appropriate testing of functional, performance, and maintenance strength before being used in live environment. The bank shall roll out the application only after closure of any critical gap found during such tests. Such tests shall also be carried out periodically in conformity with

internal / regulatory guidelines.

(2) V-CIP Procedure

- (i) Each bank shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the bank specially trained for this purpose. The official shall be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.
- (ii) Disruption of any sort including pausing of video, reconnecting calls, etc., may not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then the bank may not initiate a fresh session. However, in case of call drop / disconnection, fresh session shall be initiated.
- (iii) The bank shall vary the sequence and / or type of questions, including those indicating the liveness of the interaction, during video interactions to establish that the interactions are real-time and not pre-recorded.
- (iv) The bank shall reject the account opening process if it observes any prompting at the customer end.
- (v) The bank shall factor in the fact that the V-CIP customer is an existing or new customer, or if the case relates to one rejected earlier or if the name appears in some negative list, at an appropriate stage of workflow.
- (vi) The authorised official of the bank performing the V-CIP shall record audio and video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:
  - (a) OTP based Aadhaar e-KYC authentication.
  - (b) Offline Verification of Aadhaar for identification.
  - (c) KYC records downloaded from CKYCR, in accordance with paragraph 65, using the KYC identifier provided by the customer.
  - (d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.
- (vii) The bank shall ensure to redact or blackout the Aadhaar number in terms of paragraph 23.
- (viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the bank shall ensure that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

- (ix) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the bank shall ensure that it undertakes video process of the V-CIP within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the bank shall ensure that no incremental risk is added due to this.
- (x) If the address of the customer is different from that indicated in the OVD, the bank shall capture suitable records of the current address, as per the existing requirement. The bank shall ensure that it also confirms the economic and financial profile / information submitted by the customer from the customer undertaking the V-CIP in a suitable manner.
- (xi) The bank shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The bank shall verify the PAN details from the database of the issuing authority ,including through DigiLocker.
- (xii) The use of printed copy of equivalent e-document, including an e-PAN is not valid for the V-CIP.
- (xiii) The authorised official of the bank shall ensure that photograph of the customer in the Aadhaar / OVD and PAN / e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar / OVD and PAN / e-PAN shall match with the details provided by the customer.
- (xiv) The bank shall permit assisted V-CIP when it takes help of Business Correspondents (BCs) to facilitate the process only at the customer end. The bank shall maintain the details of the BC assisting the customer, where it utilises the services of BCs. The bank shall have the ultimate responsibility for customer due diligence.
- (xv) The bank shall make all accounts opened through V-CIP operational only after subjecting them to concurrent audit to ensure the integrity of process and its acceptability of its outcome.
- (xvi) The bank shall appropriately comply with all matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act.

### (3) V-CIP Records and Data Management

- (i) The bank shall store the entire data and recordings of V-CIP in a system / systems

located in India. The bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this direction, shall also apply to V-CIP.

- (ii) The bank shall preserve the activity log along with the credentials of the official performing the V-CIP.
28. Notwithstanding anything contained in paragraph 23 and as an alternative thereto, in case an individual who desires to open a bank account, the bank shall open a 'Small Account', which entails the following limitations:
- (1) the aggregate of all credits in a financial year does not exceed ₹one lakh;
  - (2) the aggregate of all withdrawals and transfers in a month does not exceed ₹10 thousand; and
  - (3) the balance at any point of time does not exceed ₹50 thousand.

**Provided that** the bank shall not consider this limit on balance when making deposits through Government grants, welfare benefits and payment against procurements.

- (4) Further, small accounts are subject to the following conditions:
- (i) The bank shall obtain a self-attested photograph from the customer.
  - (ii) The designated officer of the bank certifies under their signature that the person opening the account has affixed their signature or thumb impression in their presence.

**Provided that** when the individual is a prisoner in a jail, they shall affix their signature or thumbprint in the presence of the officer-in-charge of the jail and the said officer shall certify the same under his signature. The account shall remain operational only if the prisoner annually submits the proof of address that the officer in-charge of the jail issues.

- (iii) The bank shall open such accounts only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that it does not credit foreign remittances to the account.
- (iv) The bank shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before it allows a transaction to take place.
- (v) The account shall remain operational initially for a period of 12 months which the bank can extend for a further period of 12 months, provided the account

holder applies and furnishes evidence of having applied for any of the OVDs during the first 12 months of the opening of the said account.

- (vi) The bank shall review the entire relaxation provisions after 24 months.
- (vii) Notwithstanding anything contained in clauses (v) and (vi) above, the small account shall remain operational between April 1, 2020, and June 30, 2020, and such other periods as the Central Government may notify.
- (viii) The bank shall monitor the account, and when there is suspicion of money laundering or financing of terrorism activities or other high-risk scenarios, the bank shall establish the identity of the customer as per paragraph 23 or paragraphs 26 and 27.
- (ix) The bank shall not allow foreign remittance to be credited into the account unless it fully establishes the identity of the customer as per paragraph 25 or paragraph 26 and 27.

**Provided that** if the bank renders any account ineligible for being classified as a small account due to credits / balance in the account exceeding the permissible limits, the bank may allow withdrawals within the limit prescribed for small accounts where the limits thereof have not been breached.

**Further provided that** BSBD Accounts (PMJDY accounts are akin to BSBDAs), which are not KYC compliant accounts, shall be treated as 'Small Accounts' and are subjected to the limitations applicable to such accounts. Hence, for allowing normal operations in such accounts, the procedures explained above are to be complied with. If any account is rendered ineligible for being classified as a small account due to credits/balance in the account exceeding the permissible limits, withdrawals may be allowed within the limit prescribed for small accounts where the limits thereof have not been breached. If the bank renders any account ineligible for being classified as a small account due to credits / balance in the account exceeding the permissible limits, the bank may allow withdrawals within the limit prescribed for small accounts where the limits thereof have not been breached.

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

## **B. CDD Measures for Sole Proprietary firms**

30. For opening an account in the name of a sole proprietary firm, the bank shall carry out the CDD of the individual (proprietor).
31. In addition to the above, the bank shall also obtain any two of the following documents or the equivalent e-documents thereof as proof of business / activity in the name of the proprietary firm:
  - (1) Registration certificate including Udyam Registration Certificate (URC) issued by the Government.
  - (2) Certificate / licence issued by the municipal authorities under Shop and Establishment Act
  - (3) Sales and income tax returns
  - (4) CST / VAT / GST certificate
  - (5) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
  - (6) 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
  - (7) 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
  - (8) Utility bills such as electricity, water, landline telephone bills, etc.
32. In cases where the bank is satisfied that it is not possible to furnish two such documents, the bank may, at its discretion, accept only one of those documents as proof of business / activity.  
**Provided that** the bank undertakes contact point verification and collects such other information and clarifications as would be required to establish the existence of such firm, and shall confirm and satisfy itself that it has verified the business activity from the address of the proprietary concern.

## **C. CDD Measures for Legal Entities**

33. For opening an account of a company, the bank shall obtain certified copies of each of the following documents or the equivalent e-documents thereof:
  - (1) Certificate of incorporation
  - (2) Memorandum and Articles of Association

- (3) Permanent Account Number of the company
  - (4) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
  - (5) Documents, as specified in paragraph 23, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
  - (6) The names of the relevant persons holding a senior management position; and
  - (7) The registered office and the principal place of its business, if it is different.
34. For opening an account of a partnership firm, the bank shall obtain the certified copies of each of the following documents or the equivalent e-documents thereof:
- (1) Registration certificate
  - (2) Partnership deed
  - (3) Permanent Account Number of the partnership firm
  - (4) Documents, as specified in paragraph 23, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
  - (5) the names of all the partners and
  - (6) address of the registered office, and the principal place of its business, if it is different.
35. For opening an account of a trust, the bank shall obtain the certified copies of each of the following documents or the equivalent e-documents thereof:
- (1) Registration certificate
  - (2) Trust deed
  - (3) Permanent Account Number or Form No.60 of the trust
  - (4) Documents, as specified in paragraph 23, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
  - (5) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
  - (6) the address of the registered office of the trust; and
  - (7) list of trustees and documents, as specified in paragraph 23, for those discharging the role as trustee and authorised to transact on behalf of the trust.
36. For opening an account of an unincorporated association or a body of individuals, the bank shall obtain the certified copies of each of the following documents or the equivalent e-documents thereof:

- (1) Resolution of the managing body of such association or body of individuals
- (2) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
- (3) Power of attorney granted to transact on its behalf
- (4) Documents, as specified in paragraph 23, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
- (5) Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.

**Explanation:** Unregistered trusts / partnership firms shall be included under the term ‘unincorporated association’.

**Explanation:** The term ‘body of individuals’ includes societies.

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

- (1) Document showing name of the person authorised to act on behalf of the entity
- (2) Documents, as specified in paragraph 23, of the person holding an attorney to transact on its behalf and
- (3) Such documents as may be required by the bank to establish the legal existence of such an entity / juridical person.

**Provided that** in case of a trust, the bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in paragraphs 21 (2), (5), and (6) of these directions.

#### D. Identification of Beneficial Owner

38. For opening an account of a Legal Person who is not a natural person, the bank shall identify the beneficial owner(s) and shall undertake all reasonable steps in terms of sub- rule (3) of Rule 9 of the Rules to verify their identity, keeping in view the following:

- (1) Where the customer or the owner of the controlling interest is:
  - (i) an entity listed on a stock exchange in India, or
  - (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

- (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- (2) In cases of trust / nominee or fiduciary accounts, the bank determines whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. In such cases, the bank shall obtain satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.

## **E. On-going Due Diligence**

39. The bank shall undertake ongoing due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
40. Without prejudice to the generality of factors that call for close monitoring, the bank shall necessarily monitor the following types of transactions:
- (1) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
  - (2) Transactions which exceed the thresholds prescribed for specific categories of accounts.
  - (3) High account turnover inconsistent with the size of the balance maintained.
  - (4) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.
- For ongoing due diligence, the bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.
41. The bank shall align the extent of monitoring with the risk category of the customer.
- (1) The bank shall put in place a system of periodic review of risk categorisation of accounts, with such periodicity being at least once in every six months, and shall establish the need for applying enhanced due diligence measures.
  - (2) The bank shall closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) companies.

***Explanation:*** The bank shall subject high-risk accounts to more intensified monitoring.

***Explanation:*** Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing

similar amounts/dates, shall be immediately reported to RBI and other appropriate authorities such as FIU-IND.

42. Updation / Periodic Updation of KYC

- (1) The bank shall adopt a risk-based approach for periodic updation of KYC ensuring that it keeps the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, the bank shall carry out periodic updation at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every 10 years for low-risk customers from the date of opening of the account / last KYC updation. The bank shall document its policy in this regard as part of the bank's internal KYC policy duly approved by the Board of Directors of bank or any committee of the Board to which power has been delegated.
- (2) Notwithstanding the provisions given above, in respect of an individual customer who is categorised as low-risk, the bank shall allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or up to June 30, 2026, whichever is later. The bank shall subject accounts of such customers to regular monitoring. This shall also apply to low-risk individual customers for whom periodic updation of KYC has already fallen due.
- (3) Individuals:
  - (i) **No change in KYC information:** In case of no change in the KYC information, the bank shall obtain a self-declaration from the customer in this regard through the customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, or digital channels (such as online banking / internet banking, mobile application of bank) letter, etc.
  - (ii) **Change in address:** In case of a change only in the address details of the customer, the bank shall obtain a self-declaration of the new address from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter, etc., and shall verify the declared address through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.
  - (iii) Further, the bank at its option, may obtain a copy of OVD or deemed OVD, as defined in paragraph 5(1)(xiv), or the equivalent e-documents thereof, as defined in paragraph 5(1)(x), for the purpose of proof of address, declared by the customer at the time of updation / periodic updation. However, the bank

shall clearly specify such requirement, in its internal KYC policy duly approved by the Board of Directors of the bank or any committee of the Board to which power has been delegated.

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

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

The bank shall update the customer's KYC records and intimate the customer once the records get updated in the system, as required under paragraph 42(5) of the Direction. It is, however, reiterated that the concerned bank retains the ultimate responsibility for periodic updation of KYC.

- (v) Accounts of customers, who were minor at the time of opening account, on their becoming major: In case of customers for whom the bank opened an account when they were minors, the bank shall obtain fresh photographs upon their becoming a major and, at that time, shall ensure that CDD documents as per the current CDD standards are available. Wherever required, the bank may carry out fresh KYC of such customers, i.e., customers for whom it opened account when they were minor, upon their becoming a major.
- (vi) The bank may use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation. To clarify, conditions stipulated in paragraph 25 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.
- (vii) Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The bank shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any

fraud.

(4) Customers other than individuals:

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

(5) Additional measures: In addition to the above, the bank shall ensure that:

- (i) The bank has customer's KYC document as per the current CDD standards available with it. This is applicable even if there is no change in customer information but the documents available with the bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, the bank shall undertake the KYC process equivalent to that applicable for onboarding a new customer.
- (ii) The bank verifies the Customer's PAN details, if available, from the database of the issuing authority at the time of periodic updation of KYC.
- (iii) The bank provides an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, the bank shall ensure that it promptly updates the information / documents obtained from the customers at the time of updation / periodic updation of KYC in its records / database and provide an intimation, mentioning the date of updation of KYC details, to the customer.
- (iv) In order to ensure customer convenience, the bank may consider making available the facility of updation / periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of the bank or any committee of the Board to which power has been delegated.
- (v) The bank shall adopt a risk-based approach with respect to periodic updation of KYC. The bank shall clearly specify in its internal policy, duly approved by the Board of Directors of the bank or any committee of the Board to which

- power has been delegated, any additional and exceptional measures, it adopts that are not otherwise mandated under the above instructions, such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc.
- (6) The bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the bank's end.
- (7) Due Notices for Periodic Updation of KYC: The bank shall intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, the bank shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options / channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the bank shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation / reminder may, inter alia, contain easy-to-understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation / reminder shall be duly recorded in the bank's system against each customer for audit trail. The bank shall expeditiously implement the same but not later than January 01, 2026.
43. In case of existing customers, the bank shall obtain the Permanent Account Number or equivalent e-document thereof or Form No. 60, by such date which the Central Government may notify, failing which the bank shall temporarily cease operations in the account until the customer submits the Permanent Account Number or equivalent e-documents thereof or Form No. 60.

**Provided that** before temporarily ceasing operations for an account, the bank shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, the bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60

owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. However, the bank shall subject such accounts to enhanced monitoring.

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

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

## F. Enhanced and Simplified Due Diligence Procedure

### F1. Enhanced Due Diligence

44. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 25): Non-face-to-face onboarding facilitates the bank to establish a relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph include use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. The bank shall undertake the following EDD measures for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 25):

- (1) If the bank has introduced the process of V-CIP, it shall provide the same as the first option to the customer for remote onboarding. It is reiterated that the bank shall treat processes complying with prescribed standards and procedures for V-CIP on par with face-to-face CIP for the purpose of these Directions.
- (2) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. The bank shall permit transactions only from the mobile number used for account opening. The bank shall have a Board-approved policy delineating a robust process of due

- diligence for dealing with requests for change of registered mobile number.
- (3) Apart from obtaining the current address proof, the bank shall verify the current address through positive confirmation before allowing operations in the account. The bank may carry out the positive confirmation by means of such as address verification letter, contact point verification, deliverables, etc.
  - (4) The bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
  - (5) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
  - (6) The bank shall categorise such customers as high-risk customers and shall subject accounts opened in non-face-to-face mode to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.
45. Accounts of Politically Exposed Persons (PEPs)
- (1) The bank shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:
    - (i) the bank has in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
    - (ii) The bank shall take reasonable measures for establishing the source of funds / wealth;
    - (iii) the bank shall obtain approval to open an account for a PEP from the senior management;
    - (iv) the bank subjects all such accounts to enhanced monitoring on an on-going basis;
    - (v) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the bank obtains the senior management's approval to continue the business relationship;
  - (2) These instructions shall also apply to family members or close associates of PEPs.
- Explanation:** For the purpose of this paragraph, 'Politically Exposed Persons' (PEPs) are individuals who are or have been entrusted with prominent public functions **by a foreign country**, including the Heads of States / Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.
46. Client accounts opened by professional intermediaries: The bank shall ensure while opening client accounts through professional intermediaries, that:
- (1) The bank shall identify clients when a professional intermediary opens a client

- account on behalf of a single client.
- (2) The bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
  - (3) The bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality which prohibits disclosure of the client details to the bank.
  - (4) The bank shall identify all the beneficial owners where intermediaries do not co-mingle funds at the level of the bank, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the bank, the bank shall look for the beneficial owners.
  - (5) The bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
  - (6) The ultimate responsibility for knowing the customer lies with the bank.

## **F2. Simplified Due Diligence**

47. Simplified norms for Self Help Groups (SHGs):
- (1) The bank shall not require CDD of all the members of an SHG while opening the savings bank account of the SHG.
  - (2) The CDD of all the office bearers shall suffice.
  - (3) The bank may undertake CDD of all the members of an SHG at the time of credit linking of SHGs.

48. Procedure to be followed by the bank while opening accounts of foreign students
- (1) The bank shall, at its option, open a Non-Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

**Provided that** the bank shall obtain a declaration about the local address within a period of 30 days of opening the account and shall verify the said local address.

**Provided further that** pending the verification of address, the account shall be operated with the condition that allows foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of ₹50 thousand on aggregate aggregate withdrawal from the same, during the 30-day period.

- (2) The account shall be treated as a normal NRO account, and shall be operated in terms of RBI's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.
- (3) Students with Pakistani nationality shall require prior approval of the RBI for opening the account.
49. Simplified KYC norms for Foreign Portfolio Investors (FPIs):
- (1) Accounts of FPIs which are eligible / registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in (2) below, subject to Income Tax (FATCA / CRS) Rules.
- Provided that** the bank shall obtain an undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in (2) below will be submitted.
- (2) KYC documents for eligible FPIs under PIS:

|               |   | FPI Type  |   |  |
|---------------|---|---|---|--|
| Document Type |   | Category I  | Category II   | Category III                           |
| Entity Level  | Constitutive Document s (Memorandum and Articles of Association, Certificate of Incorporation etc.) | Mandatory   | Mandatory   | Mandatory                              |
|               | Proof of Address  | Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof) | Mandatory (Power of Attorney mentioning the address is acceptable as address proof) | Mandatory other than Power of Attorney |
|               | PAN   | Mandatory   | Mandatory   | Mandatory                              |

|  |                               |            |            |   |
|--|-------------------------------|------------|------------|---|
|  | Financial Data                | Exempted * | Exempted * | Mandatory   |
|  | SEBI Registration Certificate | Mandatory  | Mandatory  | Mandatory   |
|  | Board Resolution @@           | Exempted * | Mandatory  | Mandatory   |
| Senior Management<br><br>(Whole Time Directors / Partners / Trustees / etc.) | List                          | Mandatory  | Mandatory  | Mandatory   |
|  | Proof of Identity             | Exempted * | Exempted * | Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof |
|  | Proof of Address              | Exempted * | Exempted * | Declaration on Letter Head *  |

|                        |                     |  |  |                              |
|------------------------|---------------------|--|--|------------------------------|
|                        | Photographs         | Exempted   | Exempted   | Exempted *                   |
| Authorised Signatories | List and Signatures | Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian | Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian | Mandatory                    |
|                        | Proof of Identity   | Exempted *   | Exempted *   | Mandatory                    |
|                        | Proof of Address    | Exempted *   | Exempted *   | Declaration on Letter Head * |

|  | Photographs       | Exempted   | Exempted   | Exempted *                         |
|--|-------------------|------------|------------|------------------------------------|
| Ultimate<br>Beneficial<br>Owner<br>(UBO) | List              | Exempted * | Mandatory  | Mandatory                          |
|  | Proof of Identity | Exempted * | Exempted * | Mandatory                          |
|  | Proof of Address  | Exempted * | Exempted * | Declaration on<br>Letter Head<br>* |
|  | Photographs       | Exempted   | Exempted   | Exempted *                         |

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

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

| Category | Eligible Foreign Investors  |
|----------|---|
| I.       | Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organisations/ Agencies.  |
| II.      | <ul style="list-style-type: none"> <li>a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc.</li> <li>b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc.</li> <li>c) Broad based funds whose investment manager is appropriately regulated.</li> <li>d) University Funds and Pension Funds.</li> <li>e) University related Endowments already registered with SEBI as FII/Sub Account.</li> </ul> |
| III.     | All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.   |

## **Chapter VII - Record Management**

50. The bank shall take the following steps regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. The bank shall,
  - (1) 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;
  - (2) 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 has ended;
  - (3) swiftly make available, the identification records and transaction data to the competent authorities upon request;
  - (4) introduce a system of maintaining proper records of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
  - (5) maintain all necessary information in respect of transactions prescribed under PML Rule 3 to permit the reconstruction of an individual transaction, including the following:
    - (i) the nature of the transactions;
    - (ii) the amount of the transaction and the currency in which it was denominated;
    - (iii) the date on which the transaction was conducted; and
    - (iv) the parties to the transaction.
  - (6) evolve a system for proper maintenance and preservation of account information in a manner that allows the bank to retrieve data easily and quickly whenever required or when competent authorities request it;
  - (7) maintain records of the identity and address of its customers, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

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

## **Chapter VIII - Reporting Requirements to Financial Intelligence Unit – India**

52. The bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), the information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in accordance with Rule 7 thereof.

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

53. The bank shall take note of the reporting formats and comprehensive reporting format guide, prescribed / released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports. The bank which is yet to install / adopt suitable technological tools for extracting CTR / STR from its live transaction data shall make use of the editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU- IND has placed on its website. The Principal Officer of the bank, shall have suitable arrangement to cull out the transaction details from branches which are yet to be computerised and to feed the data into an electronic file with the help of the editable electronic utilities of CTR / STR as have been made available by FIU-IND on its website <http://fiuindia.gov.in>.
54. When furnishing information to the Director, FIU-IND, a delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute as a separate violation. The bank shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

The bank, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005, and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under paragraph 8 of these Directions of any analysis of transactions and activities which appear unusual, if the bank has done any such analysis.

55. To identify and report suspicious transactions effectively, the bank shall implement

robust software that generates alerts when transactions are inconsistent with a customer's risk categorisation and updated profile.

## **Chapter IX - Requirements/obligations under International Agreements -**

### **Communications from International Agencies**

56. **Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:**
- (1) The bank shall 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:
- (i) The 'ISIL (Da'esh) & Al-Qaida Sanctions List', established and maintained pursuant to Security Council resolutions 1267 / 1989 / 2253, which includes names of individuals and entities associated with Al-Qaida, is available at [www.un.org/securitycouncil/sanctions/1267/aq\\_sanctions\\_list](http://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list)
- (ii) The '**Taliban Sanctions List**', established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at <https://www.un.org/securitycouncil/sanctions/1988/materials>
- (2) The bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The bank shall verify the aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, on a daily basis, and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the bank for meticulous compliance.
- (3) The bank shall report the details of accounts resembling any of the individuals / entities in the lists to FIU-IND in addition to advising the Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 ([Annex I](#) of these Directions).

- (4) Freezing of Assets under Section 51A of UAPA, 1967: The bank shall strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 ([Annex I](#) of these Directions), and shall ensure the meticulous compliance with the Order issued by the Government. The list of Nodal Officers for UAPA is available on the website of MHA.
57. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):
- (1) The bank shall ensure meticulous compliance with the 'Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005' laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India ([Annex II](#) of these Directions).
  - (2) In accordance with paragraph 3 of the aforementioned Order, the bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
  - (3) Further, the bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
  - (4) In case of a match in the above cases, the bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under section 12A of the WMD Act, 2005. The bank shall send a copy of the communication to the State Nodal Officer, where the account / transaction is held and to the RBI.
  - (5) The bank may note that, in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.
  - (6) The bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
  - (7) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, 2005, the bank shall prevent such individual / entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
  - (8) In case the bank receives an order to freeze assets under section 12A from the CNO, the bank shall, without delay, take necessary action to comply with the Order.

- (9) The bank shall observe the process of unfreezing of funds, etc., as per paragraph 7 of the Order. Accordingly, the bank shall forward a copy of application received from an individual / entity regarding unfreezing, along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.
58. The bank shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.
59. In addition to the above, the bank shall take into account:
- (1) other UNSCRs and
  - (2) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.
60. The bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and which is accepted by the Central Government.
61. Jurisdictions that do not or insufficiently apply the FATF Recommendations
- (1) The bank shall consider the FATF Statements circulated by the RBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations. The bank shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
  - (2) The bank shall give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.
- Explanation:*** The processes referred to in (1) & (2) above do not preclude the bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.
- (3) The bank shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in

FATF Statements and countries that do not or insufficiently apply the FATF Recommendations, retain written findings together with all documents, and make them available to the RBI / other relevant authorities, on request.

62. The bank is encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

## **Chapter X - Other Instructions**

- 63. Secrecy Obligations and Sharing of Information:**
- (1) The bank shall maintain secrecy regarding the customer information that arises out of the contractual relationship between the bank and the customer.
  - (2) The bank shall treat information collected from customers for the purpose of opening of account as confidential and shall not divulge details thereof for the purpose of cross-selling, or for any other purpose without the express permission of the customer.
  - (3) While considering the requests for data / information from Government and other agencies, the bank shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
  - (4) 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) Where the interest of the bank requires disclosure, and
    - (iv) Where the disclosure is made with the express or implied consent of the customer.
- 64. Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010:** The bank shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010, and Rules made thereunder. Further, the bank shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the RBI based on advice received from the Ministry of Home Affairs, Government of India.
- 65. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)**
- (1) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

- (2) In terms of provision of Rule 9(1A) of the PML Rules, the bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- (3) Operational Guidelines for uploading the KYC data have been released by CERSAI.
- (4) The bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- (5) The 'live run' of the CKYCR started from July 15, 2016, in a phased manner, beginning with new 'individual accounts'. Accordingly, Small Finance Banks shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. SCBs were initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017.  
REs other than SCBs were required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules *ibid*.
- (6) The bank shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules *ibid*. The bank shall upload KYC records as per the LE Template released by CERSAI.
- (7) Once KYC Identifier is generated by CKYCR, the bank shall ensure that the same is communicated to the individual / LE as the case may be.
- (8) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the bank shall upload / update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (5) and (6), respectively, at the time of periodic updation as specified in paragraph 42 of these Directions, or earlier, when the updated KYC information is obtained / received from the customer. Also, whenever the bank obtains additional or updated information from any customer as per clause (10) below in this paragraph or Rule 9 (1C) of the PML Rules, the bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the bank regarding an update in the KYC record of an existing customer, the bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the bank.

- (9) The bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
- (10) For the purpose of establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, the bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless—
  - (i) there is a change in the information of the customer as existing in the records of CKYCR; or
  - (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
  - (iii) the validity period of downloaded documents has lapsed; or
  - (iv) the bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

66. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS): Under FATCA and CRS, the bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

- (1) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institutions at the link <https://incometaxindiaefiling.gov.in/> post login --> My Account --> Register as Reporting Financial Institution.
- (2) 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:*** REs shall refer to the spot reference rates published by Foreign Exchange Dealers’ Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

- (3) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
- (4) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- (5) Constitute a ‘High-Level Monitoring Committee’ under the Designated Director or

- any other equivalent functionary to ensure compliance.
- (6) Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the website <http://www.incometaxindia.gov.in/Pages/default.aspx>. REs may take note of the following:
- (i) updated Guidance Note on FATCA and CRS
  - (ii) a press release on 'Closure of Financial Accounts' under Rule 114H (8).
67. **Period for presenting payment instruments:** The bank shall not make payment of cheques / drafts / pay orders/ banker's cheques, if the customer presents them beyond the period of three months from the date of such instruments.
68. **Operation of Bank Accounts & Money Mules:** The bank shall strictly adhere to the instructions on opening of accounts and monitoring of transactions, to minimise the operations of 'Money Mules' that 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 that act as 'money mules'. The bank shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but STR was not filed by the concerned bank, it shall then be deemed that the bank has not complied with these directions.
69. **Collection of Account Payee Cheques:** The bank shall not collect account payee cheques for any person other than the payee constituent. The bank shall, at its option, collect account payee cheques drawn for an amount not exceeding ₹50 thousand to the account of its customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.
70. The bank shall allot Unique Customer Identification Code (UCIC) while entering into new relationships with individual customers as also the existing individual customers.
71. The bank shall, at their option, not issue UCIC to all walk-in / occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in

customers who have frequent transactions with them and ensure that they are allotted UCIC.

72. **Introduction of New Technologies:** The bank shall identify and assess the ML / TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products.

Further, the bank shall ensure:

- (1) to undertake the ML / TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- (2) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

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

- (1) The bank shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML / TF investigation or regulatory action. The bank shall assess the respondent bank's AML / CFT controls.
- (2) The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory / supervisory framework in the respondent bank's home country among other relevant information.
- (3) The bank shall obtain the prior approval from senior management for establishing new correspondent banking relationships. However, the bank shall also take post facto-approval of the Board or the Committee empowered for this purpose.
- (4) The bank shall clearly document and understand the respective AML / CFT responsibilities of institutions involved.
- (5) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts of the correspondent bank and is undertaking ongoing 'due diligence' on them.

- (6) The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.
- (7) The bank shall not enter into or continue a correspondent relationship with a shell bank.
- (8) The bank shall ensure that the respondent banks do not permit their accounts to be used by shell banks.
- (9) The bank shall be cautious of correspondent banking relationships with institutions located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
- (10) The bank shall ensure that respondent banks have KYC / AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

#### **74. Wire Transfer**

- (1) Information requirements for wire transfers for the purpose of this Direction:
    - (i) All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:
      - (a) name of the originator;
      - (b) the originator account number where such an account is used to process the transaction;
      - (c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
      - (d) name of the beneficiary; and
      - (e) the beneficiary account number where such an account is used to process the transaction.
- In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

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

as indicated for cross-border wire transfers in (i) and (ii) above.

- (iv) Domestic wire transfers of ₹50 thousand and above, *where the originator is not an account holder of the ordering bank*, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

In case of domestic wire transfers below ₹50 thousand where the originator is not an account holder of the ordering banks and where the information accompanying the wire transfer can be made available to the beneficiary RE and appropriate authorities by other means, it is sufficient for the ordering bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

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

- (v) The bank shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting / competent authorities as well as FIU-IND on receiving such requests with appropriate level provisions.
- (vi) The wire transfer instructions are not intended to cover the following types of payments:
- (a) Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, *for the purchase of goods or services*, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.
  - (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the

obligation of the bank to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

(2) Responsibilities of ordering bank, intermediary bank and beneficiary bank, effecting wire transfer, are as under:

(i) Ordering bank:

- (a) The ordering bank shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per sub clauses (iii) and (iv) of clause 1 above}, contain required and accurate originator information and required beneficiary information, as indicated above.
- (b) Customer Identification shall be made if a customer, who is not an account holder of the ordering bank, is intentionally structuring domestic wire transfers below ₹50 thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.
- (c) Ordering bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this paragraph.

(ii) Intermediary bank:

- (a) The bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.
- (b) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary bank.
- (c) Intermediary bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.
- (d) Intermediary bank shall have effective risk-based policies and procedures for determining:
  - a. when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
  - b. the appropriate follow-up action including seeking further information

and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

(iii) Beneficiary bank:

- (a) Beneficiary bank shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per sub clauses (iii) and (iv) of clause 1 above}, that lack required originator information or required beneficiary information.
  - (b) Beneficiary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.
- (iv) Money Transfer Service Scheme (MTSS) providers and other banks, shall comply with all of the relevant requirements of this paragraph, whether they are providing services directly or through their agents. The bank that control both the ordering and the beneficiary side of a wire transfer shall:
- (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
  - (b) file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

(3) Other Obligations

- (i) Obligations in respect of the bank's engagement or involvement with unregulated entities in the process of wire transfer: The bank shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure, *inter alia*, that:
  - (a) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
  - (b) the agreement / arrangement, if any, with such unregulated entities by the bank clearly stipulates the obligations under wire transfer instructions; and

- (c) a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.
- (ii) The bank's responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities).  
The bank is prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Directions, the bank shall ensure that they do not process cross-border transactions of designated persons and entities.
- (iii) The bank's responsibility to fulfil record management requirements: Complete originator and beneficiary information relating to wire transfers shall be preserved by the bank involved in the wire transfer, in accordance with paragraph 50 of these Directions.

75. Issue and Payment of Demand Drafts, etc.:

- (1) Any 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 ₹50 thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.
- (2) Further, the bank shall incorporate the name of the purchaser on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

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

77. Selling Third party products: The bank acting as agent while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

- (1) the identity and address of the walk-in customer shall be verified for transactions above ₹50 thousand as required under paragraph 21 (5) of these Directions.
  - (2) transaction details of sale of third-party products and related records shall be maintained as prescribed in paragraph 50 of Chapter VII.
  - (3) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
  - (4) transactions involving ₹50 thousand and above shall be undertaken only by:
    - (i) debit to customers' account or against cheques; and
    - (ii) obtaining and verifying the PAN given by the account-based as well as walk-in customers.
- (5) Instruction at (4) above shall also apply to sale of the bank's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for ₹50 thousand and above.

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

- (1) The 'at par' cheque facility offered by the bank to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.
- (2) The bank shall retain the right to verify the records maintained by the customer cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements.

79. **Issuance of Prepaid Payment Instruments (PPIs):** PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

80. Hiring of Employees and Employee training:

- (1) The bank shall put in place an adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of its personnel recruitment / hiring process.
- (2) The bank shall endeavour to ensure that the staff dealing with / being deployed for KYC / AML / CFT matters have: high integrity and ethical standards, good understanding of extant KYC / AML / CFT standards, effective communication skills

and ability to keep up with the changing KYC / AML / CFT landscape, nationally and internationally. The bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

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

## **Chapter XI - Repeal and Other Provisions**

### **81. Repeal and saving**

- (1) With the issue of these Directions, the existing Directions, instructions, and guidelines relating to Know Your Customers as applicable to Small Finance Banks stand repealed, as communicated vide notification dated XX, 2025. The Directions, instructions, and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.
- (2) Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed Directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions.

### **82. Application of other laws not barred**

The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or directions, for the time being in force.

### **83. Interpretation:**

For the purpose of giving effect to the provisions of these Directions or in order to remove any difficulties in the application or interpretation of the provisions of these Directions, the RBI may, if it considers necessary, issue necessary clarifications in respect of any matter covered herein and the interpretation of any provision of these Directions given by the RBI shall be final and binding.

## **Annex I**

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

North Block, New Delhi.

Dated: the 2<sup>nd</sup> February, 2021

(Amended vide corrigendum dated March 15, 2023) (Amended vide corrigendum dated August 29, 2023)  
(Amended vide corrigendum dated April 22, 2024)

### **ORDER**

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

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

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

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

The Unlawful Activities (Prevention) Act, 1967 defines ‘Order’ as under: - ‘Order’ means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

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

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

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

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

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

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

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

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

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

4.1 The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988

Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA.

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

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

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

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

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

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

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

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

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

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

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

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

6.6 Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the

Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

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

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

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

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

(iii) The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organisations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organisation, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laid down in the paragraphs 6.2 to 6.5 above. The Registrar should also be advised that no

societies/ firms/ non-profit organisations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in turn, follow the procedure laid down in the paragraphs 6.2 to 6.5 above.

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

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

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

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

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

of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

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

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

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

8.2 To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

8.3 The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation, 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 authorise, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

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

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

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

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

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

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

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

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

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

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

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

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

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

Officers of all States/UTs.

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

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

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

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

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

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

(  
A  
s  
h

utosh Agnihotri)

Joint Secretary to the Government of India

To,

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

Copy for information to: -

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

**Annex II**  
**F.No.P - 12011/14/2022-ES Cell-DOR**

**Government of India**  
**Ministry of Finance**  
**Department of Revenue**

\*\*\*

**New Delhi, dated the 1<sup>st</sup> September, 2023**

**ORDER**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

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

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

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

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

2.3 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other

organisations concerned, for initiating verification and suitable action.

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

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

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

3.1 All Financial Institutions shall –

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

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

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

iv. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section

12A, REs shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post , without delay.

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

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

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

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

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

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

ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. In case, the designated individuals/entities are holding financial assets or

economic resources of the nature of immovable property, and if any match with the designated individuals/entities is found, the Registrar shall immediately inform the details with full particulars of the assets or economic resources involved *to* the State Nodal Officer, without delay.

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

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

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

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

4.5 In case, the results of the verification indicate that the assets are owned by, or are

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

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

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

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

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in

the paragraphs 4.2 to 4.6 above. The Registrar should also ensure that no societies/ firms/ non-profit organizations should be allowed to be registered if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and, in case, such request is received, then the Registrar shall inform the State Nodal Officer, without delay.

(iii) The State Nodal Officer shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

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

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

(vi) In addition, a member of the ICSI shall, if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

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

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

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

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

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

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

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

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

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including FIs and DNFBPs obligated to carry out sanctions screening. The concerned

Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

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

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO to be: -

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

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

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

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

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

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

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

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

- (i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;
- (ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and
- (iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization

**7. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the individual or entity is not a designated person or no longer meet the criteria for designation:**

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

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

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services,

owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

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

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

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

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

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

(Manoj Kumar Singh)  
Director (HQ)

To,

- 1) Governor, Reserve Bank of India, Mumbai
- 2) Chairman, Securities & Exchange Board of India, Mumbai

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

Copy for information to: -

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

