

ASSAM GRAMIN VIKASH BANK

Know Your Customer (KYC) Policy, 2024-25

(Updated as per RBI's Master Direction on KYC updated as on January 04, 2024 and Amendment to the Master Direction - Know Your Customer (KYC) Direction, 2016 dated November 06, 2024)

(Annex to Circular No. AGVB/P&D/26/OM-146/2024-25 dated 21-11-2024)



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, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Aadhaar and other Laws (amendment) Ordinance, 2019 as notified by the Government of India, Bank is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

This KYC Policy is issued as per RBI's Master Directions on Know Your Customer (updated as on 04-01-2024) which incorporates the amendments made by Government of India, vide Gazette Notification G.S.R. 582(E) dated August 19, 2019 and Gazette Notification G.S.R. 840(E) dated November 13, 2019.

All offices of the Bank shall take all necessary steps to implement this KYC policy and provisions of Prevention of Money- Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

CHAPTER – I : Preliminary

1. Short Title

Policy guidelines on Know Your Customer (KYC) Norms / Anti Money laundering (AML) Standards / Combating of Financing of terrorism (CFT) Measures / Obligation of the Bank under Prevention of Money Laundering Act (PMLA), 2002 shall be called as Know Your Customer (KYC) Policy, 2024-25.

2. Applicability

(a) The provisions of KYC Policy guidelines shall apply to all the branches / offices of the Bank.

3. Definitions

In terms of RBI's Master Direction on KYC, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

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

- i. **"Aadhaar number"** as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

"Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
- ii. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
- iii. **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv. **Beneficial Owner (BO)**

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

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of / entitlement to more than 25 per cent of the shares or capital or profits of the company.

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

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

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

- d. **Where the customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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 of OVD"** - Obtaining a certified copy by bank shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Branch under his EPF Number with remark "Verified with Original. Branch Official will also attest the duly signed photograph of the customer.

- 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 designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. A person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Regional Rural Banks.

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

- ix. **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000). [Presently, as per Information Technology Act, 2000, Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000]

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

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

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



- xiii. **"Non-profit organisations"** (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).
- xiv. **"Officially valid document"** (OVD) means the Passport, the Driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, Job Card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,
- a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
 - b. Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-
 - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post- paid mobile phone, piped gas, water bill);
 - ii. property or Municipal tax receipt;
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation.
 - c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
- Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.
- xv. **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016)
- xvi. **"Person"** has the same meaning assigned in the Act and includes:
- a. an individual,
 - b. Hindu undivided family,
 - c. a company,
 - d. a firm,
 - e. an association of persons or a body of individuals, whether incorporated or not,
 - f. every artificial juridical person, not falling within any one of the above persons (a to e), and
 - g. any agency, office, or branch owned or controlled by any of the above persons (a to f).
- xvii. **"Principal Officer"** means an officer at the management level nominated by the Bank, 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 offense specified in the Schedule to the Act, regardless of the value involved; or
 - b. appears to be made in circumstances of unusual or unjustified complexity; or
 - c. appears to not have an economic rationale or bona-fide purpose; or
 - d. gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be



linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism

- 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 Section 16.
- xx. "**Transaction**" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
- opening of an account;
 - 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;
 - the use of a safety deposit box or any other form of safe deposit;
 - entering into any fiduciary relationship;
 - any payment made or received, in whole or in part, for any contractual or other legal obligation; or
 - establishing or creating a legal person or legal arrangement.
- xxi. "**UCIC**" means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

(B) Terms bearing meaning assigned in RBI Master Directions on KYC, unless the context otherwise requires, shall bear the meanings assigned to them below:

- "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.
- "Walk-in Customer" means a person who does not have an account based relationship with the Bank, but undertakes transactions with the Bank.
- "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

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

- 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;
 - Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
 - 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.
- "Customer identification" means undertaking the process of CDD.
 - "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
 - "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of Bank.
 - "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that those are consistent with Bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.
 - "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank."
 - "Video based Customer Identification Process (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Bank by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification



information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of the Master Direction on KYC.

x. "Wire transfer" related definitions:

- a. **Batch transfer:** Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.
- b. **Beneficiary:** Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
- c. **Beneficiary Regulated Entity:** It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary Regulated Entity and makes the funds available to the beneficiary.
- d. **Cover Payment:** Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
- e. **Cross-border wire transfer:** Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
- f. **Domestic wire transfer:** Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
- g. **Financial Institution:** In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
- h. **Intermediary Regulated Entity:** Intermediary Regulated Entity refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
- i. **Ordering Regulated Entity:** Ordering Regulated Entity refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
- j. **Originator:** Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
- k. **Serial Payment:** Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).
- l. **Straight-through Processing:** Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.
- m. **Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.



- n. Wire transfer: Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.
- xi. **"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.
- xii. "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
- xiii. "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.
- xiv. "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.

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

CHAPTER - II : General

4. RBI has advised the Bank that a Know Your Customer (KYC) Policy, duly approved by the Board of Directors of the Bank, be formulated and put in place.

4.1. Purpose

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

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

4.2. Objective

The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:

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

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

5. The KYC policy includes following four key elements:

- (a) Customer Acceptance Policy (CAP);
- (b) Risk Management;
- (c) Customer Identification Procedures (CIP); and
- (d) Monitoring of Transactions

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

- (a) 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise to be carried out 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 should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Bank from time to time.

- (b) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. STR/CTR will form an integral part of the assessment process and the outcome of the identified parameters shall be placed before the Risk Committee of the Board for vetting. The periodicity of risk assessment exercise shall be in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
 - (c) Risk Management Department shall carry out the above said Risk Assessment exercise on annual basis. The Compliance Cell of the Bank will be assigned with the responsibility for ensuring compliance to the approved policy guidelines besides generation, preparation and submission of the statutory reports like CTR, STR and Counterfeit Transaction, etc. to the appropriate authority. The outcome of the exercise shall be put up to the Risk Management Committee of the Board and should be available to competent authorities and self-regulating bodies.
- 5B.** Bank shall apply a Risk Based Approach(RBA) for mitigation and management of the identified risk in line with the Board approved policies, controls and procedures in this regard. Bank shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, Bank shall monitor the implementation of the controls and enhance them, if necessary.

6. Designated Director:

- (a) An Executive Director on the Board to be nominated as "Designated Director", as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. Designated Director shall be nominated by the Board.
- (b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
- (c) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
- (d) In no case, the Principal Officer be nominated as the 'Designated Director'.

7. Principal Officer:

- (a) The General Manager, Planning & Development Dept. has been nominated as the Principal Officer of the Bank, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law / regulations.
- (b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
- (c) The Principal Officer will report to Designated Director and will oversee the functioning of Centralised AML Cell as per PML Act/ KYC Policy.
- (d) The Principal Officer will maintain close liaison with enforcement agencies, banks and other institutions which are involved in the fight against money laundering and combating financing of terrorism.
- (e) Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

8. Compliance of KYC policy:

- (a) Compliance with KYC Policy is to be ensured through:
 - i. A senior officer in the rank of General Manager who will constitute as 'Senior Management' for the purpose of KYC compliance.
 - ii. Allocation of responsibility through Office Order for effective implementation of policies and procedures at HO / Regional Offices/Other Controlling Offices level.
 - iii. All HO Divisions to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
 - iv. Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Inspection & Audit Department, HO.
 - v. Concurrent / internal audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and

Know Your Customer (KYC) Policy, 2024-25



compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.

- vi. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports during branch inspection.
- (b) It is to be ensured that decision-making functions of determining compliance with KYC norms are not outsourced by the bank.
- (c) The implementation of KYC-AML guidelines by branches in letter and spirit, has to be ensured by Regional Managers /Controlling Heads/Officials and the same is to be checked during their visit to branches.

CHAPTER – III : Customer Acceptance Policy

9. A Customer Acceptance Policy has been framed by the bank, as under-

10. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, it is to be ensured that:

- (a) Customer acquisition will be limited to Resident Indian only.
- (b) No account is opened in anonymous or fictitious / benami name.
- (c) No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. The Bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- (d) No transaction or account based relationship is undertaken without following the CDD procedure.
- (e) The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
- (f) Additional information, where such information requirement has not been specified in the internal KYC Policy of the Bank, is obtained with the explicit consent of the customer.
- (g) The CDD procedure is to be applied at the UCIC level. Thus, if an existing KYC compliant customer of Bank desires to open another account with the same Bank, there shall be no need for a fresh CDD exercise.
- (h) CDD Procedure is followed for all the joint account holders, while opening a joint account.
- (i) Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
- (j) No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
- (k) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- (l) Where an equivalent e-document is obtained from the customer, Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- (m) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

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

12. 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

13. For Risk Management, Bank has adopted risk based approach which includes the following.

- a. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the Bank.
- b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and information about the clients' business and their location etc. **While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.**

It is hereby specified that the various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.



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

CHAPTER – V : Customer Identification Procedure (CIP)

14. Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:
- Commencement of an account-based relationship with the customer.
 - The customer shall produce any other acceptable documents (other than OVD) as Identity and Address proof
 - When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
 - Selling third party products as agent, selling its own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than rupees fifty thousand.
 - Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
 - When Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
 - It is to be ensured that introduction is not to be sought while opening accounts.
15. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank, will at its option, rely on customer due diligence done by a third party, subject to the following conditions:
- Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
 - Adequate steps are taken by Bank to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
 - The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
 - The third party shall not be based in a country or jurisdiction assessed as high risk.
 - The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

CHAPTER – VI : Customer Due Diligence (CDD) Procedure

Part I -CDD Procedure in case of Individuals

16. For undertaking CDD, concerned offices 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:
- the Aadhaar number where,
 - he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - he decides to submit his Aadhaar number voluntarily to the bank; or
 - the proof of possession of Aadhaar number where offline verification can be carried out; or
 - the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
 - the KYC Identifier with an explicit consent to download records from CKYCR; and
 - the Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, and
 - one recent photograph; and
 - such other documents including in respect of the nature of business and financial status of the customer, as may be required



by the Bank:

Provided that where the customer has submitted,

- i. Aadhaar number under clause (a) above, authentication of the customer's Aadhaar number to be carried out using e-KYC authentication facility provided by the Unique Identification Authority of India.
Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.
- ii. proof of possession of Aadhaar under clause (a) above where offline verification can be carried out, the Bank shall carry out offline verification.
- iii. an equivalent e-document of any OVD, the Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo under Digital KYC Process. The Digital KYC Process in case of our Bank will be implemented through Sponsor Bank as per guidelines laid down in Master Direction on KYC issued by RBI.
- iv. any OVD or proof of possession of Aadhaar number under clause (b) above where offline verification cannot be carried out, the Bank shall carry out verification through digital KYC.
- v. KYC Identifier under clause (c) above, the Bank shall retrieve the KYC records online from the CKYCR in accordance with Section 53.

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

Explanation 1: Branch/Offices shall, where its customer submits his proof of possession of Aadhaar Number containing Aadhaar Number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

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

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

While establishing an account based relationship with individual customer, the branch official to ascertain as to whether the customer is already having a Customer ID with the Bank. In case the customer has an existing Customer ID, fresh Customer ID shall not be created and the new account shall be opened with the existing Customer ID.

The name, father's name, date of birth and address of the customer be filled in the same manner and style as it appears in the KYC document provided by the customer. Branch official will ensure that all the mandatory fields in Account Opening Form / Customer Master Form (marked as *) such as Name, Fathers" name , date of birth, address , Identity Proof , address proof, Identification number (Identity proof document number) , Profession / activity (Nature of Business- specific) , total annual income , total annual turnover (in case of business) etc. are completely and correctly filled in by the customer and are also correctly captured in customer's database in CBS. The respective division/ offices of the Bank shall ensure that branches are capturing correct data in CBS system, particularly in respect of Constitution Code, Profession/ Activity, Occupation, Income/ Turnover etc. as risk category of the customer is assigned on the basis of these parameters.

In case of High Risk Customers, the authenticity of the OVD should be should be verified through respective On- line portal.

17. Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

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



- ii. As a risk-mitigating measure for such accounts, Bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Bank shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.
- iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
- vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Regulated Entity(RE). Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Regulated Entities shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- ix. Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

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

- i) CDD in case of new customer on-boarding 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, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 22 and Section 22A, apart from undertaking CDD of the proprietor.

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

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

(a) V-CIP Infrastructure: Bank shall undertake V-CIP through Sponsor Bank and shall adhere to the following minimum standards of V-CIP Infrastructure as detailed in Master Direction on KYC updated from time to time.

(b) V-CIP Procedure

- i) Bank shall formulate a clear work flow and standard operating procedure for V-CIP through ORMC as per Master Direction on KYC updated from time to time and thereby ensure adherence to it. The V-CIP process shall be operated by officials of the Bank specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(c) V-CIP Records and Data Management

The entire data and recordings of V-CIP shall be stored in a system / systems located in India and the same will be provided through Sponsor Bank. The extant instructions on record management, as stipulated in the RBI's Master Direction on KYC updated from time to time, shall also be applicable for V-CIP.

19. Notwithstanding anything contained in Section 16 and as an alternative thereto, in case an individual who desires to open a bank account, bank shall open a 'Small Account', which entails the following limitations:

- (i) the aggregate of all credits in a financial year does not exceed Rupees one lakh;
- (ii) the aggregate of all withdrawals and transfers in a month does not exceed Rupees ten thousand; and
- (iii) the balance at any point of time does not exceed Rupees fifty thousand.

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

Further, small accounts are subject to the following conditions:



- a) A self-attested photograph to be obtained from the customer.
- b) The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
- c) Such accounts are opened only at Core Banking Solution (CBS) linked branches/BC Points to ensure that foreign remittances are not credited to the account.
- d) It is to be ensured that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
- e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
- f) The entire relaxation provisions shall be reviewed after twenty four months.
- g) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high-risk scenarios, the identity of the customer shall be established.

20. 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 full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Part II - CDD Measures for Sole Proprietary firms

- 21.** For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.
- 22.** In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business / activity in the name of the proprietary firm shall also be obtained:

- (i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
- (ii) Certificate / Licence issued by the municipal authorities under Shop and Establishment Act.
- (iii) Sales and income tax returns.
- (iv) CST / VAT / GST certificate (provisional / final).
- (v) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
- (vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- (vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities.
- (viii) Utility bills such as electricity, water, and landline telephone bills.

22 A. In cases where the concerned office is satisfied that it is not possible to furnish two such documents, the concerned office may, at their discretion, accept only one of those documents as proof of business / activity. Provided it undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Legal Entities

- 23. For opening an account of a company,** certified copies of each of the following documents shall be obtained:

- (i) Certificate of incorporation;
- (ii) Memorandum and Articles of Association;
- (iii) Permanent Account Number of the company;
- (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
- (v) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
- (vi) the names of the relevant persons holding senior management position; and
- (vii) the registered office and the principal place of its business, if it is different.



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

- (i) Registration certificate;
- (ii) Partnership deed;
- (iii) Permanent Account Number of the partnership firm; and
- (iv) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
- (v) the names of all the partners and
- (vi) address of the registered office, and the principal place of its business, if it is different.

25. For opening an account of a trust, certified copies of each of the following documents shall be obtained:

- (i) Registration certificate;
- (ii) Trust deed;
- (iii) Permanent Account Number or Form No.60 of the trust; and
- (iv) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
- (v) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
- (vi) the address of the registered office of the trust; and
- (vii) list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

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

- (i) Resolution of the managing body of such association or body of individuals;
 - (ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
 - (iii) Power of attorney granted to transact on its behalf;
 - (iv) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
 - (v) such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.
- Explanation: Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.

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

- (i) Document showing name of the person authorised to act on behalf of the entity;
- (ii) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and
- (iii) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

28. For opening an account of Hindu Undivided Family, certified copies of each of the following documents shall be obtained :

- (i) Identification information as mentioned under Section 16 in respect of the Karta and Major Coparceners,
- (ii) Declaration of HUF and its Karta,
- (iii) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
- (iv) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

Provided that in case of a trust, Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (e) and (f) of Section 14 of this MD.

Part IV - Identification of Beneficial Owner

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

- (a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in



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

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

Part V - On-going Due Diligence

30. On-going due diligence of customers to be undertaken to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds / wealth.

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

- (a) 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.
- (b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
- (c) High account turnover inconsistent with the size of the balance maintained.
- (d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

32. The extent of monitoring shall be aligned with the risk category of the customer. Explanation: High risk accounts have to be subjected to more intensified monitoring.

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

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

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

33. Updation / Periodic Updation of KYC

A risk-based approach is adopted by the Bank for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

(a) Individual Customers:

i. **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through post/ by visiting the base branch, provided validity of the OVD is not expired.

ii. **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through post/ by visiting the base branch and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Such requests must contain the signature of the account holder and a copy of the self-attested OVD should be enclosed.

iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the base branch. Wherever required, branch may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major. As the KYC documents are to be maintained at base branch, the customer may contact his/her base branch.

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

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

(b) Customers other than individuals:



i. **No change in KYC information:** In case of no change in the KYC information of the Legal Entity (LE) customer, a self- declaration (letter from an official authorized by the LE in this regard, board resolution etc.) in this regard shall be obtained from the LE customer through its email id registered with the Bank/ by post/ by visiting the base branch. Further, branch shall ensure during this process that Beneficial Ownership (BO)/Authorised Signatories information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible. In case of Company accounts, one Board resolution should accompany the request.

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

(c) Additional measures: In addition to the above, it shall be ensured by the concerned offices that,

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

(d) In case of existing business relationship which is not KYC compliant, operations in the account to be temporarily ceased. However, before temporarily ceasing operations for an account, it is to be ensured to give the client one notice (through Letter/SMS or any other electronic form) and within 30 days period the account should be made KYC compliant otherwise operations in the account shall be frozen. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

(e) Branches shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit 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 Banks' end.

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

Provided that before temporarily ceasing operations for an account, the client is to be given an accessible notice (through Letter/SMS or any other electronic form) and a reasonable opportunity to be heard.

However, operations in accounts of 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, may allowed to be continued. The Branch Head shall allow such relaxation for continuation of operations in such accounts till the time PAN or Form 60 is obtained from the customer for which an officer from the branch will be deputed to personally visit the customer for obtaining the PAN or Form 60. However, the Branch Head shall ensure that such accounts are subject 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 he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

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

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

35. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17): Non-face-to-face onboarding facilitates Bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc. Following EDD measures shall be undertaken by Bank for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):



36. Accounts of Politically Exposed Persons (PEPs)

- (a) The Branch/offices shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that apart from performing normal customer due diligence: :
- (i) Bank shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
 - (ii) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
 - (iii) the identity of the person shall have been verified before accepting the PEP as a customer;
 - (iv) the decision to open an account for a PEP is taken at a senior level, i.e. at the level of **Regional Office** and above, in accordance with the Bank's Customer Acceptance Policy;
 - (v) all such accounts are subjected to enhanced monitoring on an on-going basis;
 - (vi) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
 - (vii) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
- (b) These instructions shall also be applicable to accounts where a PEP is the beneficial owner, family members or close associates of PEPs. Explanation: For the purpose of this Section, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

37. Client accounts opened by professional intermediaries:

While opening client accounts through professional intermediaries, it is to be ensured that:

- (a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (b) Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- (c) Accounts of such professional intermediaries not to be opened, who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
- (d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the concerned office shall look for the beneficial owners.
- (e) The offices 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.
- (f) The ultimate responsibility for knowing the customer lies with the Bank.

B. Simplified Due Diligence

38. Simplified norms for Self Help Groups (SHGs)

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

CHAPTER - VII : Record Management

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

- (a) maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction;
- (b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;



(c) make available swiftly the identification records and transaction data to the competent authorities upon request;
(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following :

- (i) the nature of the transactions;
- (ii) the amount of the transaction and the currency in which it was denominated;
- (iii) the date on which the transaction was conducted; and
- (iv) the parties to the transaction.

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

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

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

39A. Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

CHAPTER - VIII : Reporting Requirements to Financial Intelligence Unit – India

40. The concerned office shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

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

41. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Bank in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Bank which are yet to install/adopt suitable technological tools for extracting CTR / STR from their live transaction data.

42. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Offices shall not put any restriction on operations in the accounts where an STR has been filed and shall keep the fact of furnishing of STR strictly confidential. It is to be ensured that there is no tipping off to the customer at any level.

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

44. Reports to be furnished to Financial Intelligence Unit – India.

(1) Cash Transaction Report (CTR).

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

(ii) The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

(iii) A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through MIS Report: Misc Reports Module under



(2) Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, bank is to be guided by the definition of “suspicious transaction” as contained in PMLA Rules as amended from time to time.

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

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

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

(ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted transactions in STRs to be reported, even if not completed by the customers, irrespective of the amount of the transaction.

(iii) STR to be submitted if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) Furnishing of STR to be ensured within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

(v) It shall be ensured not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.

(vi) The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions. Controlling offices shall monitor transactions in customer accounts, in general, and high risk accounts/ high value transactions, in particular.

(vii) For effective monitoring of transactions of the customers, Bank has implemented an AML system for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. Further, an indicative list of behavioural/observation based scenarios has been circulated vide Centralized AML Cell (FRMD) Circular No. 01/2021 dated 22.01.2021. In case any suspicious transaction is detected, the same be reported to Centralised AML Cell for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FINnet Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators i.e. customer behaviour and risk based transaction monitoring, high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at Annexure- II.

(3) Counterfeit Currency Report (CCR)

Cash transactions where forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit- India in the specified format by 15th of the succeeding month.

45. Internal Control System

i. **Centralized AML Cell:** Monitoring, analysis & closure of AML alerts, including Trade Based Money Laundering (TBML) alerts, shall be done at Centralized AML Cell on day to day basis. Makers/ Checkers at Centralized AML Cell will analyze alerts on day to day basis and will close the alerts after thorough analysis of the transactions/ alerts and ensuring that all the transactions are genuine in nature & match with the business profile of customers. Post-closure scrutiny of closed alerts (@20%) shall be undertaken at Centralized AML Cell.



STRs on all suspicious transactions shall be put up to Principal Officer immediately for approval and onward submission to FIU-IND. Similarly, STRs on adverse media reports, Law Enforcement Agency enquiries etc. shall also be prepared and put up to Principal Officer.

During analysis of alerts, special attention shall be given to alerts pertaining to TBML, High Risk Customers, Politically Exposed Persons & High Value Transactions.

- ii. Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members. Senior Officers from the Zonal / Circle / Regional Offices, during their visits to the branches will ensure that KYC / AML guidelines are being strictly adhered to as per the laid down procedures, keeping in view the risk involved in a transaction, account or banking/business relationship.
- iii. For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data and other Customer Due Diligence information, transaction records and other relevant information.
- iv. Any changes in KYC Policy, on account of amendments made by RBI in its Master Direction on KYC, shall be immediately adopted by the Bank and circular shall be issued. The information regarding such change shall be placed before Board on regular basis for information/ratification.

CHAPTER – IX : Requirements / Obligations under International Agreements

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

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

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>

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

<https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl>

It is to be ensured that 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 is also referred.

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

48. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions / entities from time to time shall also be taken note of.

49. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated February 2, 2021 (Annexure-III) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

(a) Offices 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 III of this Master Direction).

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

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



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

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

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

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

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

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded 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.

51. The 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, should be verified 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.\

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

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

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

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

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

Explanation: The process referred to in Section 52 a & b do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

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

CHAPTER – X : Other Instructions

53. Secrecy Obligations and Sharing of Information:

(a) All offices shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

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

(c) The exceptions to the said rule shall be as under :

i. Where disclosure is under compulsion of law,



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

(d) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer

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

(a) 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.

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

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

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

(e) Post implementation and live run of the CKYCR, concerned offices are required to invariably upload the KYC data pertaining to all new individual accounts opened.

(f) KYC records pertaining to accounts of LEs opened on or after April 1, 2023 have to be uploaded, with CKYCR in terms of the provisions of the Rules *ibid*. The KYC records have to be uploaded as per the LE Template released by CERSAI.

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

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the concerned office shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 36 of this KYC Policy, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Bank obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9(1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updating of KYC record of the said customer. Once CKYCR informs the Bank regarding an update in the KYC record of an existing customer, Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank.

(i) it is to be ensured that during periodic updation, the customers are migrated to the current CDD standard.

(j) Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to the Bank, with an explicit consent to download records from CKYCR, then concerned office shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless

-
- (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 Bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client; or
- (iv) the validity period of documents downloaded from CKYCR has lapsed.

54A. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, **Head Office of Bank** shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and shall take following steps for complying with the reporting requirements:

(a) 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,

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure



for the purposes of identifying reportable accounts in terms of Rule 114H.

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

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

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

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

(i) updated Guidance Note on FATCA and CRS

(ii) press release on 'Closure of Financial Accounts' under Rule 114H (8).

Branches must ensure the following:

(i) **For New Accounts:** The properly filled and signed FATCA/ CRS declaration forms are invariably required to be taken with all the new Account Opening forms and details of all the declared / derived FATCA / CRS reportable accounts should be properly recorded in Finacle CRM module in the "Tax Certification Details" Tab.

(ii) **For Existing Accounts:** It is also mandatory to insist for FATCA / CRS declarations from the existing account holders and if the present FATCA / CRS reportable status is changed, the details of the same should also be properly updated in the Finacle CRM module in "Tax Certification Details" Tab. Since FATCA / CRS is an ongoing process, if there is any change in the account information, the Branch may be required to contact the customer to obtain additional information / documentation and also update its customer account classification under FATCA / CRS.

The Declaration Forms for the new accounts shall be stored along with the opening forms whereas, the Declaration Forms taken for the existing account holders should be stored in a separate file for proper record keeping.

55. Period for presenting payment instruments

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

56. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules. Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the bank, it shall be deemed that the concerned office/s has/ve not complied with these directions.

57. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected.

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

b) It is to be ensured not to issue UCIC to all walk-in / occasional customers such as buyers of pre-paid instruments /purchasers of third party products. However, UCIC shall be allotted to such walk-in customers who have frequent transactions.

59. Introduction of New Technologies - Credit Cards / Debit Cards / Smart Cards / Gift Cards / Mobile Wallet / Net Banking / Mobile Banking / RTGS / NEFT / ECS / IMPS etc.

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

Know Your Customer (KYC) Policy, 2024-25



services / technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

60. Issue and Payment of Demand Drafts, etc.

Any remittance of funds by way of demand draft, mail / telegraphic transfer / NEFT / IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

61. Quoting of PAN

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

62. Selling Third party products

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

(a) the identity and address of the walk-in customer shall be verified for transactions above Rupees fifty thousand as required under Section 14(e) of this Directions.

(b) transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 38.

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

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

- 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.

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

63. Issuance of Prepaid Payment Instruments (PPIs):

It is to be ensured that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

64. Hiring of Employees and Employee training

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

(b) Bank shall 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. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(c) On-going employee training programme shall be put in place 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 front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC / AML / CFT policies of the Bank, regulation and related issues shall be ensured.

XXXXXXXXXXXXXXXXXX



**INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS I.E. CUSTOMER BEHAVIOUR AND RISK BASED TRANSACTION MONITORING,
HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/ LOCATIONS/ALERTS FOR BRANCHES/ OFFICES**

1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

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

A. Transactions Involving Large Amounts of Cash

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

B. Transactions that do not make Economic Sense

- i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
- ii. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

C. Activities not consistent with the Customer's Business

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



D. Attempts to avoid Reporting/Record-keeping Requirements

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

E. Unusual Activities

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

F. Customer who provides Insufficient or Suspicious Information

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

G. Certain Suspicious Funds Transfer Activities

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

H. Certain Bank Employees arousing Suspicion

- i. An employee whose lavish lifestyle cannot be supported by his or her salary.
- ii. Negligence of employees/willful blindness is reported repeatedly.

I. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

J. Some examples of suspicious activities/transactions to be monitored by the operating staff.

- i. Large Cash Transactions
- ii. Multiple accounts under the same name
- iii. Frequently converting large amounts of currency from small to large denomination notes
- iv. Placing funds in term Deposits and using them as security for more loans.
- v. Large deposits immediately followed by wire transfers.
- vi. Sudden surge in activity level.
- vii. Same funds being moved repeatedly among several accounts.
- viii. Multiple deposits of money orders, Banker's cheques, drafts of third Parties
- ix. Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
- x. Cheques of third parties into the account followed by immediate cash withdrawals.
- xi. Transactions inconsistent with the purpose of the account.
- xii. Maintaining a low or overdrawn balance with high activity



Check list for preventing money-laundering activities:

- i. A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- ii. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
- iii. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
- iv. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- v. A customer experiences increased wire activity when previously there has been no regular wire activity.
- vi. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- vii. A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
- viii. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- ix. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- x. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- xi. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- xii. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- xiii. Periodic wire transfers from a person's account/s to Bank haven countries.
- xiv. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- xv. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travellers cheques
- xvi. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when the amount is very large (say over Rs.10 lakhs), the amount is just under a specified threshold, the funds come from a foreign country or such transactions occur repeatedly.
- xvii. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)
- xviii. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

2. INDICATIVE LIST OF HIGH RISK CUSTOMERS

- i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban*
- ii. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities*
- iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
- iv. Customers with dubious reputation as per public information locally available or commercially available.
- v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
- vi. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
- vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
- viii. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
- ix. Non-resident customers and foreign nationals
- x. Accounts of Embassies / Consulates;
- xi. Off-shore (foreign) corporation/business



- xii. Non face-to-face customers
- xiii. High net worth individuals [HNIs]
- xiv. Firms with 'sleeping partners'
- xv. Companies having close family shareholding or beneficial ownership
- xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
- xvii. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence
- xviii. Investment Management / Money Management Company/Personal Investment Company
- xix. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
- xx. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fundmanagers, trustees, custodians, etc
- xxi. Trusts, charities, NGOs/NPOs (especially those operating on a "crossborder" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
- xxii. Money Service Business: including seller of: Money Orders / Traveller's" Checks / Money Transmission /CheckCashing / Currency Dealing or Exchange
- xxiii. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
- xxiv. Gambling/gaming including "Junket Operators" arranging gambling tours
- xxv. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
- xxvi. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
- xxvii. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
- xxviii. Customers that may appear to be Multi-level marketing companies etc.

**No fresh account to be opened if name appears in the list. However, if any existing account is placed in the list subsequently, the same shall be freezed and placed in high risk till its final closure.*

3. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

- i. Non-Bank Financial Institution
- ii. Stock brokerage
- iii. Import / Export
- iv. Gas Station
- v. Car / Boat / Plane Dealership
- vi. Electronics (wholesale)
- vii. Travel agency
- viii. Used car sales
- ix. Telemarketers
- x. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
- xi. Dot-com company or internet business
- xii. Pawnshops
- xiii. Auctioneers
- xiv. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
- xv. Sole Practitioners or Law Firms (small, little known)
- xvi. Notaries (small, little known)
- xvii. Secretarial Firms (small, little known)
- xviii. Accountants (small, little known firms)
- xix. Venture capital companies



4. LIST OF HIGH / MEDIUM RISK PRODUCTS & SERVICES

- i. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers(domestic and international), etc
- ii. Electronic banking
- iii. Private banking (domestic and international)
- iv. Trust and asset management services
- v. Monetary instruments such as Travelers' Cheque
- vi. Foreign correspondent accounts
- vii. Trade finance (such as letters of credit)
- viii. Special use or concentration accounts
- ix. Lending activities, particularly loans secured by cash collateral and marketable securities
- x. Non-deposit account services such as Non-deposit investment products and Insurance
- xi. Transactions undertaken for non-account holders (occasional customers)
- xii. Provision of safe custody and safety deposit boxes
- xiii. Currency exchange transactions
- xiv. Project financing of sensitive industries in high-risk jurisdictions
- xv. Trade finance services and transactions involving high-risk jurisdictions
- xvi. Services offering anonymity or involving third parties
- xvii. Services involving banknote and precious metal trading and delivery
- xviii. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS / COUNTRIES

Countries / Jurisdictions

- i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR").
- ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatfgafi.org)
- iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
- iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
- v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.
- vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- vii. Countries identified by credible sources as having significant levels of criminal activity.
- viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations

- i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
- ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
- iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

5. INDICATIVE LIST OF HIGH RISK COUNTRIES:

The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.



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

North Block, New Delhi.
Dated: the 2nd February, 2021

[\(Amended vide corrigendum dated March 15, 2023\)](#)

[\(Amended vide corrigendum dated August 29, 2023\)](#)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1 The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries



Know Your Customer (KYC) Policy, 2024-25

regulated by the SEBI and insurance companies requiring them -

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.6 Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the



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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

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 III
F.No.P - 12011/14/2022-ES Cell-DOR
Government of India
Ministry of Finance
Department of Revenue

New Delhi, dated the 1st September, 2023.

ORDER

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

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

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

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

- a) freeze, seize or attach funds or other financial assets or economic resources—
 - i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or
 - ii. held by or on behalf of, or at the direction of, such person; or
 - iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;
- prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

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

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

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

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

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

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

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

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

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

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

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

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will



Know Your Customer (KYC) Policy, 2024-25

maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

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

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

3.1 All Financial Institutions shall –

- i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, 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 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 transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, he unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization

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

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

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



7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

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

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

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

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

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

(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)

