
[Registered Office: G.B. Pant Road, Nainital, Uttarakhand-263001]
CIN No. U65923UR1922PLC000234, website: www.nainitalbank.co.in
e-mail ID: cs@nainitalbank.co.in, Phone: 05942-233739

# Know Your Customer (KYC)

# and

# Anti-Money Laundering (AML)Policy

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

## DOCUMENT CONTROL

| | |
|---|---|
| **Ownership** | **Operations Department** |
| **Title** | **KYC and AML Policy** |
| **Date of Approval** | 29.07.2023 |
| **Classification** | **Public** |
| **Periodicity** | 12 months |
| **Review** | June 24,2024 |

## TABLE OF CONTENTS


| CLAUSE | CONTENTS | PAGE NO. |
|---|---|---|
| **1.** | Preamble | 2 |
| **2.** | Objective | 2 |
| **3.** | Scope | 2 |
| **4.** | Chapter-I: Preliminary | 3 |
| **5.** | Chapter-II: General | 12 |
| **6.** | Chapter-III: Customer Acceptance Policy | 16 |
| **7.** | Chapter –IV: Risk Management | 18 |
| **8.** | Chapter- V: Customer Identification Procedure (CIP) | 22 |
| **9.** | Chapter- VI: Customer Due Diligence (CDD) Procedure | 24 |
| **10.** | Chapter-VII: Record Management | 38 |
| **11.** | Chapter-VIII: Reporting Requirements to Financial Intelligence Unit - India | 39 |
| **12.** | Chapter-IX: Requirements/obligations under International Agreements- Communications from International Agencies | 43 |
| **13.** | Chapter-X: Other Instructions | 45 |
| **14.** | Annexure-1: Digital KYC Process | 54 |
| **15.** | Annexure 2: Procedure for implementation of Section 51A of the Unlawful (Prevention) Act, 1967 | 56 |
| **16.** | Annex III: Order | 65 |
| **17.** | Annexure IV: High & Medium Risk: Customers/ Products & Services/ Geographies/ Locations/Alerts For Branches/ Offices | 73 |
| **18.** | Annexure V: Risk Categorisation | 80 |
| **19.** | Applicability | 81 |
| **20.** | Periodicity of review of Policy | 81 |

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

## 1. Preamble

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

- 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.

- 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.

## 2. Objective

The purpose of KYC policy is to put in place customer identification procedures for opening of accountsand 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.

## 3. Scope

In terms of the 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 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 updated Directions on Know Your Customers guidelines. 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).

The provisions of this Know Your Customer Policy shall apply to all the branches / offices of the Bank.

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

# Chapter-I: Preliminary

In terms of the 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 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 updated Directions on Know Your Customers guidelines. 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).

**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, 2020**.

**2. Applicability**

The provisions of this Know Your Customer Policy shall apply to all the branches / offices of the Bank.

**3. Definitions**

As per the RBI 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 thePrevention of Money-Laundering (Maintenance of Records) Rules, 2005:**

i) "**Aadhaar numbe**r" 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 10 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 shareholder's agreements or voting agreements.

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

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

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

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

e) **Exemption from Identification of Beneficial Owner:** It is not necessary to identify and verify the identity of any stakeholder or beneficial owner in the following entities as provided in PML Rule 2005:

- Any entity listed in stock exchanges in India.
- An entity resident in jurisdiction notified by the Central Government and listed on stock exchanges in such jurisdictions.
- A subsidiary of such listed entities.

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

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)},

alternatively, the original certified copy, certified by any one of the following, may be obtained:

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

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 to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and the Rules shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.
g. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
h. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
i. In no case, the Principal Officer shall be nominated as the 'Designated Director

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

viii) **"Digital KYC"** means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officeras 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). (at present, 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) **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

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

xiii) **"Officially Valid Document"** (OVD) means:

- Passport,
- Driving licence
- Proof of possession of Aadhaar number
- 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.
- Letter issued by the National Population Register containing details of name and address.

Provided that,

i. 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.

ii. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address.
   a. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
   b. property or Municipal tax receipt;
   c. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
   d. 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 officialaccommodation;

iii. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

iv. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter

issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

xiv) **"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).

xv) **"Person"** has the same meaning assigned in the Act and includes:

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

xvi) **"Principal Officer"** means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

i. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
ii. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
iii. Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

xvii) **"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 offencespecified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activitiesrelating 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.

xviii) A **"Small Account"** means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005.

xix) **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangementthereof and includes:

a. opening of an account;

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

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

xxi) **"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.

**(B) Terms bearing meaning assigned in Master Directions of Reserve Bank of India on KYC, unless thecontext otherwise requires, shall bear the meanings assigned to them below:**

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

ii. **"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.

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

iv. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.

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

vi. **"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.

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

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

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

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

xi. **"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.

xii. **"Politically Exposed Persons"** (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

xiii. **"Shell bank"** means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xiv. **"Wire transfer"** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means witha view to making an amount of money available to a beneficiary person at a bank. **"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 RE: 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 RE 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 RE: Intermediary RE 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 RE: Ordering RE refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

j. Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the 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 means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means witha view to making an amount of money available to a beneficiary person at a bank.

xv. **"Domestic and cross-border wire transfer":** When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

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

to-face CIP for the purpose of this Master Direction.

xvii. "Regulated Entities" (REs) means

a. All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'
b. All India Financial Institutions (AIFIs)
c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator

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

xix. **"Correspondent Banking":** Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the 10 "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable through accounts and foreign exchange services.

(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 14Aadhaar (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 usedin commercial parlance, as the case may be**.

## Chapter-II: General

4. In terms of the Reserve Bank of India Master Directions this policy is a " Know Your Customer" (KYC) policy duly approved by the Board of Directors.

5. Bank shall ensure that a group-wide policy is implemented for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003).

6. This Policy ensure the framework of the bank for compliance with PML Act/Rules, including regulatory instructions in this regard which provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, Bank will consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

7. Additional information, where such information requirement has not been specified in the KYC Policy of the bank shall be obtained with the explicit consent of the customer.

8. The Deduplication and Blacklisting of customer should be carried out invariably in CBS to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of this MD. The AML application of the bank scans the name of existing customer with that of the sanction list on an ongoing basis.

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

### 10. 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.

### 11. Objective

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

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

know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.

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

**12. The KYC policy includes the following four key elements:**

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

**13. Designated Director**

To ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules the **MD and CEO** of the bank is nominated as" Designated Director "by the Board and the name, designation and address of the Designated Director is communicated to the FIU-IND.

**14. Principal Officer**

The **General Manager and "The Chief Operating Officer**" of the bank, posted at Head Office, Seven Oaks, Mallital, Nainital is designated as Principal Officer. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer is communicated to the FIU-IND.

In case The General Manager and **"The Chief Operating Officer"** of the bank is absent due to valid reasons, a senior management officer equivalent to the rank of **Vice President** posted at the Banks Head Office will act as an Alternate Principal Officer to ensure timely compliance.

**15. Compliance of KYC policy:**

(a) Bank shall ensure compliance with KYC Policy through:

i. A senior officer in the rank of AVP/VP who will constitute as 'Senior Management 'for the purpose of KYC compliance.
ii. Allocation of responsibility through Office Order for effective implementation of policiesand procedures at HO / RO level.
iii. All HO Departments to ensure compliance of KYC guidelines in their respective areas ofoperations.
iv. Independent evaluation of the compliance functions of Bank's policies and procedures, including legal and regulatory requirements be done by Compliance Department at 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. Atthe end of every calendar quarter, implementation and 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 from EDW / CBS.

(b) Bank shall carry out periodical ML/TF Risk Assessment periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countriesor geographic areas, products, services, transactions or delivery channels, etc. The risk assessment shall-

I. be conducted once in a year in the month of April.
II. follow Risk based approach
III. be documented;
IV. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
V. be kept up to date; and
VI. be reported to the Audit Committee of the Board
VII. be available to competent authorities and self-regulating bodies.

(c) Bank shall ensure that decision-making functions of determining compliance with KYC norms are notoutsourced.

(d) The implementation of KYC-AML guidelines by branches in letter and spirit has to be ensured byRegional heads and the same is to be checked during their visit to branches.

**16. Money Laundering and Terrorist Financing Risk Assessment by Bank:**

(a) Bank carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise on annual basis through its Central Internal Audit Division (CIAD).

(b) The objective of such assessment is:

- 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 share with REs from time to time.

(c) The risk assessment by the CIAD, be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the bank.

(d) Further, the periodicity of risk assessment exercise shall be determined by the Board of the bank,

in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

(f) Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, REs shall monitor the implementation of the controls and enhance them if necessary.

(g) The risk assessment shall include-

I. be conducted once in a year in the month of April to June.
II. follow Risk based approach
III. be documented;
IV. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
V. be kept up to date; and
VI. be reported to the Audit Committee of the Board
VII. be available to competent authorities and self-regulating bodies.

(h) Bank's decision-making functions of determining compliance with KYC norms are notoutsourced.

(i) The implementation of KYC-AML guidelines by branches in letter and spirit has to be ensured by Regional heads and the same is to be checked during their visit to branches

## Chapter-III: Customer Acceptance Policy

**17.** Bank 's Customer Acceptance Policy ensures that:

a. **No account is opened in anonymous or fictitious/benami name-** No account should be opened where the bank is unable to verify the identity and/or obtain documents required or non-reliability of the data/information furnished to the bank to apply appropriate CDD measures, either due to non - cooperation of the customer or non-reliabity of the documents/ information furnished by the customer.

b. **No account is opened where the Bank is unable to apply appropriate CDD measures, either dueto non-cooperation of the customer or non-reliability of the documents/information furnishedby the customer-** Before opening a new account, it should be ensured that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. The Branches should refer the circulars issued by RBI/Government of India/Central Office from time to time wherein the names of banned/terrorist individuals/organization etc. are notified. The name(s) of the prospective customer should be verified with the latest —banned/sanctioned List by undergoing blacklist scanning in CBS.

c. **No transaction or account-based relationship is undertaken without following the CDD procedure-** In cases where the customer is permitted to act on behalf of another person/entity the circumstances should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

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

**e. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.**

f. **Bank shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Bank desires to open another account, there shall be no need for a fresh CDD exercise-** the bank has issued circular for De-duplication and branches should ensure that no duplication CIF should be opened.

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

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

i. **Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India-** Branches must check for Black list scanning in CBS.

**j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the**

**verification facility of the issuing authority.**

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

18. **Risk Categorization of Customers:** Customers shall be categorized as low, medium and highrisk category, based on the assessment and risk perception. The branches should preparethe profile of the customer which should contain information relating to customers' identity, social/financial status, nature of business activity, information about his clients' business and their location etc. and risk categorization shall be undertaken based on these parameters. The Bank has automated the process of Risk Categorization through AML Application and conduct it in every six months.

19. Additional information, where such information requirement has not been specified in the in this policy, is obtained with the explicit consent of the customer.

20. The Blacklisting procedure in CBS ensures that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists. Further the AML application of the bank scans the names of existing customer on an on-going basis to ensure identity of the customer do not match with the sanctioned list.

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

22. Bank ensure that 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. One such account is small account.

23. In case of suspicion of money laundering or terrorist financing, and it reasonably believed that performing the CDD process will tip-off the customer, bank/branch shall not pursue the CDD process, and instead file an STR with FIU-IND.

Bank shall ensure that 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.

# Chapter –IV: Risk Management

**24.** For Risk Management, the Bank have a risk based approach which includes the following.

I. Customers shall be categorised as low, medium and high risk category, based on the assessmentand risk perception.

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

III. The risk categorisation of a customer and the specific reasons for such categorisation will be kept confidential and not be revealed to the customer to avoid tipping off the customer.

IV. FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), and other agencies, etc., shall also be used in risk assessment.

V. The customer profile shall be prepared based on risk categorization, as defined below:

**i. Low Risk Category**

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.

Example:

(a) Salaried Employees, whose salary structures are well defined,

(b) People belonging to lower economic strata of the Society whose accounts show small balances and low turnover,

(c) Government departments and Government owned Companies, Regulators and statutory bodies etc.

(d) All other Customers who are not classified as High Risk or Medium Risk Categories

For low risk category customers, only the basic requirements of verifying the identity and location of the customer are to be obtained. However, whenever there is suspicious of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact pose a low risk, full scale customer due diligence should be carried out before opening an account or whenever such risk perceived.

**ii. Medium Risk Category:**

Those individuals who live in Medium risk Countries i.e. all Countries in Africa and all countries in the America other than USA and Canada and Such customers who possess lower risk than High Risk Customers but higher than the Low Risk Customers based on their background, nature and location of activity, country of origin, sources of funds etc. The Risk Classification may be lower for those customers where sufficient knowledge in the public domain is available to Bank (e.g. listed companies, Regulated Entities).

**iii. High Risk Category:**

Individuals and entities whose identities and sources of funds are not clear and cannot be easily identified

Indicative List of Medium Risk Customers – Annexure-IV. Its hereby specified that various other information collected from different categories of customersrelating to the perceived risk, is non-intrusive.

VI. For High Risk Category & Medium Risk Category customers, the Enhanced Due Diligence (EDD) be done by taking the information such as customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. should be obtained. There should be periodical review of risk categorization of accounts followed by enhanced due diligence measures. Such review of risk categorization of customers should be carried out at least once in every six months.

VII. Branch may take a view on risk categorization of each customer into low, medium and high risk category depending on their experience, expertise in profiling of the customer based on their understanding, judgment, assessment and risk perception of the customer and not merely based on any group or class they belong to.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

**25.** Broad Principles and System of periodic review of risk categorization of accounts:

In consideration of above, Bank conduct such assessment of risk categorization of customers on a half yearly basis. The parameter for risk assessment taken into consideration includes nature of activity and transaction trends in the last six months. This procedure was followed in the bank prior to CBS migration.

With the up gradation of CBS, bank implemented new Anti-Money Laundering (AML) software with enhanced facilities. One such facility is automation of risk categorization process. The new AML Software will categorize the risk taking into consideration following parameters:

1. KYC/ Business Intelligence Risk
2. Transaction Trend/Pattern Risk
3. Transaction Type Risk
4. Scenario/Rule Risk Violation Risk

**26. Periodical Updation of KYC:**

Periodic updation of KYC of customer is 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.

In terms to amendment to Section 38 of Master Direction on KYC, the following procedure is to be adopted for Re-KYC i.e., Periodic updation of KYC of customers:

i) For Individual Customers Risk – based approach for periodic updation of KYC is to be adopted:
   - 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.
   - 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 and the declared address shall be verified by sending registered letter.

- 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 branches. Wherever required, branches 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.
- Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 of RBI's MD on KYC are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Bank shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud

ii) For Customers other than individuals Risk – based approach for periodic updation of KYC is to be adopted:

- No change in KYC information: In case of no change in the KYC information of the Legal Entity (LE) customer, a letter from an official authorized by the LE in this regard, board resolution etc. should be obtained by the branches. Further, branches shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.
- Change in KYC information: In case of change in KYC information, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

**27. Additional measures:**

In addition to the above, branches shall ensure that,

i) The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the branch 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, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

ii) Customer's PAN and Aadhaar details, if available with the branch, must be verified from the database of the issuing authority at the time of periodic updation of KYC.

iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

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

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 to the branch the update of such documents. This shall be done within 30 days of the update to the documents for the

purpose of updating the records at bank's end.

**28. Cessation of account for non-submission of Periodical Updation of KYC:**

In case of existing customers, where the KYC documents are not obtained, by such date as may be notified by the Central Government, then branches shall temporarily cease operations in the account till the time KYC documents is submitted by the customer. Provided that before temporarily ceasing operations for an account, branches shall give the customer an accessible notice and a reasonable opportunity to be heard. There is relaxation for continued operation of accounts for customers who are unable to provide KYC documents owing to injury, illness or infirmity on account of old age or otherwise and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

If a customer having an existing account-based relationship with a branch gives in writing to the branch that he does not want to submit his KYC documents, branch 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.

**29. Evaluation and Ensuring the Adherence to the KYC policies and procedures:**

Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. Concurrent/ Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard and inform the respective branch which will take immediate action for rectification of the reported irregularities. The compliance in this regard placed before the Audit Committee of the Board on quarterly intervals.

**30.** The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

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

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

a. Commencement of an account-based relationship with the customer.
b. Carrying out any international money transfer operations for a person who is not an account holder of the bank.
c. When there is a doubt about the authenticity or adequacy of the customer identificationdata obtained.
d. Selling third party products as agents, selling 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.
e. Carrying out transactions for a non-account-based customer, that is a walk-in customer,where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
f. When the Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold ofrupees fifty thousand.
g. Bank shall ensure that introduction is not to be sought while opening accounts.

**32.** For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank shall at its option, rely on customer due diligence done by a third party, subject to the following conditions:

a. 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.
b. Adequate steps are taken by Bank to satisfy 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.
c. 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.
d. The third party shall not be based in a country or jurisdiction assessed as high risk.
e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

**33. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, bank may rely on customer due diligence done by a third party, subject to the following conditions:**

i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
ii. Adequate steps shall be taken by bank to satisfy themselves 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.
iii. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the

requirements and obligations under the PML Act.

iv. The third party shall not be based in a country or jurisdiction assessed as high risk.

v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.

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

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

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

(a) the Aadhaar number where,

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

II. he decides to submit his Aadhaar number voluntarily to the bank; or

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

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

(ac) the KYC Identifier with an explicit consent to download records from CKYCR;

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined inIncome-tax Rules, 1962; and

(c) one recent photograph; and

(d) At least one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status, annual income, turnover (in case of business) such as salary slip, Registration certificate, Certificate / licence issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence / certificate of practice issued by any professional body incorporated under a statue, Complete Income Tax Returns (Not just the acknowledgement) and Registration certificate including Udyam Registration Certificate (URC) issued by the Government. etc . However, customers who don't have business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in un-organized sector, farmers etc may submit self-declaration to this effect.

Provided that where the customer has submitted,

a. Aadhaar number under clause (a) above, the bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. 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

b. Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.

c. an equivalent e-document of any OVD, the Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

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

e. KYC Identifier under clause (ac) above, the RE shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

f. When Aadhaar number is received from customers,

- Branches may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India (UIDAI).
- The branch shall carry out offline verification where offline verification can be carried out on the proof of possession of Aadhaar. Offline verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the regulations of Income Tax Department and UIDAI.

Provided that for a period not beyond such date as may be notified by the Government for a class of Banks, instead of carrying out digital KYC, the Bank may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 9 of the policy. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

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

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

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

While establishing an account based relationship with individual customer, the branch official to ascertain as to whether the customer is already having a CIF ID with the Bank through De-duplication process in CBS. In case the customer hasan existing CIF ID, fresh CIF ID shall not be created and the new account shall be opened with the existing CIF ID.

The name, father's name, date of birth and address of the customer be filled in the same manner andstyle 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 such as Name, Father's 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 Regional 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 onthe basis of these parameters.

In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain. PAN Card and Voter Identity Card, wherever obtained, be verified on-line through the respective websites and a print of on-line verification of the said document be held on record with the relevant AOF.

Branches 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 KYC Identifier with an explicit consent to download records from CKYCR.

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

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

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

v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 15 is to be carried out.

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

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

viii) 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.

ix) Following Risk mitigating measure for such account has been added in the process:

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 account

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

i) The official of the Bank performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information either using OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may also be used by bank for aiding the V-CIP.

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

iii) Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India.

iv) The official of the Bank shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v) The official of the Bank shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

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

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

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

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

x) The audiovisual interaction shall be triggered from the domain of the Bank itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi) Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii) Bank will take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Bank.

xiii) Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 15.

xiv) BCs can facilitate the process only at the customer end and as already stated above, the official atthe other end of V-CIP interaction should necessarily be a bank official. Bank shall maintain thedetails of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

xv) 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 Master Direction on KYC.

**37.** Notwithstanding anything contained in Section 15 and as an alternative thereto, in case an individual who desires to open a bank account, banks shall open a 'Small Account', which entails the following limitations:

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

ii. the aggregate of all 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

Governmentgrants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

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

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

C. 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.

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

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

F. 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.

G. The entire relaxation provisions shall be reviewed after twenty-four months.

H. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be establishedas per Section 15.

I. Foreign remittance shall not be allowed to be credited into the account unless the identity of thecustomer is fully established as per Section 15.

**Part II CDD Measures for Sole Proprietary Firms**

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

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

ii. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

iii. Sales and income tax returns.

iv. (provisional/final). CST/VAT/ GST certificate

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 or 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, landline telephone bills, etc.

**ix.** The following document is added as a proof of business/ activity in the name of the proprietary firm:

- Registration certificate including Udyam Registration Certificate (URC) issued by the Government.

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

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

**Part III- CDD Measures for Legal Entities**

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

i. Certificate of incorporation

ii. Memorandum and Articles of Association

iii. Permanent Account Number of the company

iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

v. Documents, as specified in Section 15, 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;

**vii.** the registered office and the principal place of its business, if it is different.

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

i. Registration certificate

ii. Partnership deed

iii. Permanent Account Number of the partnership firm

iv. Documents, as specified in Section 15, relating to names of all the partners

v. beneficial owner, managers, officers oremployees, as the case may be, holding an attorney to transact on its behalf.

vi. the registered office and the principal place of its business, if it is different.

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

i. Registration certificate

ii. Trust deed
iii. Permanent Account Number or Form No.60 of the trust
iv. Documents, as specified in Section 16 of RBI's Master Direction of KYC (Know Your Customer), 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 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 of RBI's Master Direction of KYC (Know Your Customer), for those discharging the role as trustee and authorized to transact on behalf of the trust.

**42.** For opening an account of an unincorporated association or a body of individuals, certified copies ofeach of the following documents or the equivalent e-documents thereof shall be obtained:
a. Resolution of the managing body of such association or body of individuals
b. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
c. Power of attorney granted to transact on its behalf
d. relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and Documents, as specified in Section 15,
e. Such information as may be required by the Bank to collectively establish the legal existence ofsuch 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.

**43.** For opening accounts **of juridical persons 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 there of shall be obtained:**

a. Document showing name of the person authorized to act on behalf of the entity;
b. Documents, as specified in Section 16 of RBI's Master Direction of KYC (Know Your Customer) of the person holding an attorney to transact on its behalf and
c. Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

**Part IV -Identification of Beneficial Owner**

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

a. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
b. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of

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

c. **Controlling Ownership Interest:**

The threshold limit for controlling ownership interest for the purpose of determination of Beneficial Owner in case of both Companies and Trust has been revised to 10% from earlier threshold of 25% and 15% respectively (as per amendment RBI's Master Direction (MD) on KYC (Know Your Customer) dated February 25, 2016, Reserve Bank of India vide circular dated April 28,2023).

d. 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.

**Part V - On-going Due Diligence**

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

**46.** 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.

e. Bank will explore possibilities for adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring as a part of ongoing due diligence.

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

**Explanation**: High risk accounts will 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 Multi-Level 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.

**48. Periodic Updation**

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 as per the following procedure:

**(a) Individuals:**

i) **No change in KYC information:** In case of no change in the KYC information, a self-declaration from the customer shall be obtained through customer's email-id registered with the bank or through registered post.

ii) **Change in address:** In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank or through registered post and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter/ letter of thanks etc.

Further, bank shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of Master Direction on KYC AML , for the purpose of proof of address, declared by the customer at the time of periodic updation.

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

iv) Aadhaar OTP based e-KYC in non-face to face mode may be used for 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. REs 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 customer, a self-declaration in this regard shall be obtained from the Legal Entity customer through its email id registered with the bank, letter from an official authorized by the Legal Entity in this regard, board resolution, etc. Further, bank shall ensure that during this process that Beneficial Ownership (BO) information available with them is accurate and shall be updated to keep it as up-to-date as possible.

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

**(c) Additional measures**: In addition to the above, bank/branch shall ensure that:

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

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

iii) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv) As a measure of risk-based approach with respect to periodic updation of KYC branch shall obtain recent photograph, require physical presence of the customer, periodic updation of KYC only in the branch where account is maintained.

**(d)** The following instruction on obligation of customers in terms of requirements of PML Rules is added:

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 to the branch, the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.

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

Provided that before temporarily ceasing operations for an account, the Bank shall give the customer an accessible notice and a reasonable opportunity to be heard.

Further, Branch head may allow for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes If feasible an officer of the branch should be deputed to obtain such documents from the customer personally Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with Bank gives in writing that he does not want to submit his Permanent Account Number or equivalent e-document thereofor 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 creditsshall be allowed.

**Part VI - Enhanced and Simplified Due Diligence Procedure**

**A. Enhanced Due Diligence**

**50. Accounts of non-face-to-face customers (other than Aadhaar OTP based on- boarding):** Non-face-to-face onboarding facilitates the banks 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., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by banks for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

- In case bank introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face Customer Identification Process for the purpose of this Master Direction.
- In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Bank have a due process of due diligence for dealing with requests for change of registered mobile number.
- Apart from obtaining the current address proof, bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter/ letter of thanks, contact point verification, deliverables, etc.
- Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP
- Bank shall ensure that the first payment is to be effected through the customer's KYC- complied account with another Bank, for enhanced due diligence of non-face-to-face customers.

**51. Accounts of Politically Exposed Persons (PEPs)**

**A.** Bank shall have the option of establishing a relationship with PEPs provided that:

a. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

b. the identity of the person shall have been verified before accepting the PEP as a customer;

c. the decision to open an account for a PEP is taken at Regional Office.

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

e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, Regional Offices' approval is obtained to continue the business relationship;

f. the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis areapplicable.

**B.** These instructions shall also be applicable to accounts where a PEP is the beneficial owner

**52.** Client accounts opened by professional intermediaries:

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

a. Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
b. Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c. Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank,
d. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the Bank shall look for the beneficial owners.
e. Bank shall, at it's 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.

**C. Simplified Due Diligence**

**53.** Simplified norms for Self Help Groups (SHGs)
(a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
(b) CDD of all the office bearers shall suffice.
(c) CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs

**54. Procedure to be followed while opening accounts of foreign students**

(a) Bank shall, at its option, open a Non Resident Ordinary (NRO) bank account of a foreign student onthe basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter

offering admission from the educational institution in India.

i. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

ii. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

(b) The account shall be treated as a normal NRO account, and shall be operated in terms of ReserveBank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.

(c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening theaccount.

**55.** Simplified KYC norms for Foreign Portfolio Investors (FPIs) Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex IV, subject to Income Tax (FATCA/CRS) Rules.
Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex IV will be submitted.

# Chapter-VII: Record Management

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

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

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

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

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

v. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so asto permit reconstruction of individual transaction, including the following:

   a. the nature of the transactions;
   b. the amount of the transaction and the currency in which it was denominated;
   c. the date on which the transaction was conducted; and
   d. the parties to the transaction.

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

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

Explanation. – For the purpose of this 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 Chapter VIII Reporting Requirements to Financial Intelligence Unit – India

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

## Chapter-VIII: Reporting Requirements to Financial Intelligence Unit - India

**58.** Bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred toin 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 amendmentto 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 about the form of furnishing information and to specify the procedure and the manner of furnishing information.

**59.** The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Bank which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those REs, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the helpof the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website https://www.fingate.gov.in.

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

**61.** 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.

**62. Reports to be furnished to Financial Intelligence Unit – India.**

- **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 seriesof 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 will be available at the concerned branch for production to auditors/Inspectors, when asked for.

- **Suspicious Transaction Reports (STR)**

i. While determining suspicious transactions, bank will 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 goodfaith:

**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. Bank will report all such attempted transactionsin STRs, even if not completed by the customers, irrespective of the amount of the transaction.

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

v. 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 officials of 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.

vi. 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. 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 behavior and risk based transaction monitoring, high & medium risk: customers/ products & services/ geographies/ locations/alerts for branches/ departments, are attached at **Annexure III.**

- **Counterfeit Currency Report (CCR)**

Cash transactions were forged or counterfeit currency notes have been used as genuine or where

any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.

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

- **Cross-border Wire Transfer [CWTR]**
  Bank will file Cross-Border Wire Transfer Report (CWTR) to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

**63. Internal Control System**

**a.** Regional Heads be designated as Nodal Officer for compliance of KYC Policy in all branches under its jurisdiction. He will ensure that field functionaries are sensitized on KYC / AML guidelines and ensure that no money laundering activities take place in the branches under his/her jurisdiction. For this purpose, he/she should also ensure on-site supervision by visiting the branches under his/her jurisdiction for random checking of compliance of KYC / AML guidelines of the Bank.

**b.** **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. AML Official at Centralized AML Cell will analyze alerts pertaining to their respective assigned Regionson 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. They will also ensure that necessary corrective steps are initiated for the discrepancies observed during sample checking. 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, and Politically Exposed Persons & High Value Transactions.

Incumbent In-charge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members. Senior Officers from the Regional\Head Office, 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.

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.

Any changes in KYC Policy may be implemented after approval of the Board.

**Function of Central AML Cell**

i. Transaction Monitoring through AML application
ii. Maintenance and development/customization of AML application in liaison with RDC and the system Vendor
iii. Timely submission of reports to FIU-IND Viz., CTR, STR, CCR, NTR etc.
iv. KYC/AML Inspection Reports
v. Train the staff on KYC/AML guidelines

**c. Inspection Department**

i. Conducting Regular, Concurrent and Special KYC audits.

**d. Regional Offices:**

i. Oversight of compliance of KYC/AML guidelines by branches
ii. Following up and ensuring full rectification of deficiencies in KYC/AML compliance reported in various Inspections.

**e. Compliance Function**

i. Evaluating and ensuring adherence to the KYC policies and procedures (based on KYC
ii. Inspection reports) by the branches.
iii. Independent evaluation of the bank's own KYC/AML/CFT policies and procedures visa-vislegal and regulatory requirements.

# Chapter-IX: Requirements/obligations under International Agreements- Communications from International Agencies

**64. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967**

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

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

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

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

iii. 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 (MHA) as required under UAPA notification dated February 2, 2021 (Annex II of this Master Direction).

iv. Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

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

(a) REs 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 January 30, 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, REs shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

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

(d) In case of match in the above cases, REs 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. REs shall file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) REs 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, REs 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 REs from the CNO, REs shall, without delay, take necessary action to comply with the Order.

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

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

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

**68.** 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 processes referred to in (a) & (b) above do not preclude REs 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.

**69.** Bank shall explore the possibilities to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements

# Chapter-X: Other Instructions

**70. Secrecy Obligations and Sharing of Information:**

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

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

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

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

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

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

Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

Bank shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. SCBs were, however, allowed time upto February 1, 2017 for uploading date in respect of accounts opened during January 2017.
Further, since the CKYCR is now fully operational for individual customers, it has been decided to extend the CKYCR to Legal Entities (LEs). Accordingly, bank shall upload the KYC data pertaining to accounts of LEs opened on or after April 1, 2021, on to CKYCR in terms of Rule 9 (1A) of the Rules.

In order to ensure that all existing KYC records of individual customers are incrementally uploadedon to CKYCR, bank shall upload the KYC data pertaining to accounts of individuals opened prior to January 01, 2017, at the time of periodic updation as specified in Section 38 of the Master Direction, or earlier when the updated KYC information is obtained/received from the customer in certain cases.
Bank shall ensure that during periodic updation, the customers' KYC details are migrated to currentCDD standard.
Where a customer, for the purpose of establishing an account based relationship, submits a KYC Identifier to a bank, with an explicit consent to download records from CKYCR, then bank shall retrieve the KYC records online from 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;(ii)the current address of the customer is required to be verified;

(iii) the bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

Once KYC Identifier is generated by CKYCR, the bank shall ensure that the same is communicated tothe individual/legal entity as the case may be.

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

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

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

(b) Submit online reports by using the digital signature ofthe '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 forrecording 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 114Hof Income Tax Rules.

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

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

i. updated Guidance Note on FATCA and CRS
ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

**73. Period for presenting payment instruments**

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

**74. 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." If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

**75. Collection of Account Payee Cheques**

Account payee cheques for any person other than the payee constituent shall not be collected. Bank shall, at its option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of its customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

**76.** (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) The bank shall, at it's option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

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

Bank shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Further, bank shall ensure:

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

**78. Correspondent Banks**

Bank shall have a policy approved by the Boards, or by a committee headed by the MD & CEO to lay down parameters for approving correspondent banking relationships subject to the following conditions:

(a) Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.
(b) Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.
(c) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.

(d) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts andis undertaking on-going 'due diligence' on them.

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

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

(g) It shall be ensured that the correspondent banks do not permit their accounts to be used byshell banks.

(h) Bank shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

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

**79. Wire transfer**

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

Bank shall ensure the following while effecting wire transfer:

**i.** All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such:

- name of the originator;
- the originator account number where such an account is used to process the transaction;
- the originator's address, or national identity number, or customer
- identification number, or date and place of birth;
- name of the beneficiary; and
- the beneficiary account number where such an account is used to
- process the transaction.

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

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

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

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

**v.** REs shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

**vi.** The wire transfer instructions are not intended to cover the following types of payments:

a. Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

b. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

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

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

**viii.** Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR **shall be made to FIU-IND.**

**ix.** Complete originator information relating to qualifying wire transfers shall be preserved at leastfor a period of five years.

**x.** If processing as an intermediary element of a chain of wire transfers Bank shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

**xi.** The receiving intermediary bank shall transfer full originator information accompanying a cross- border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

**xii.** All the information on the originator of wire transfers shall be immediately made available toappropriate law enforcement and/or prosecutorial authorities on receiving such requests.

**xiii.** Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place as a beneficiary bank.

**xiv.** As a Beneficiary Bank shall report transaction lacking complete originator information toFIU-IND as a suspicious transaction.

**xv.** As a beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the Bank shall consider restricting or terminating its business relationship with the ordering bank.

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

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

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

iii. Beneficiary RE:
   a. Beneficiary RE shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify crossborder wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.
   b. Beneficiary RE shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iv. Money Transfer Service Scheme (MTSS) providers are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. In the case of a MTSS provider that controls both the ordering and

the beneficiary side of a wire transfer, the MTSS provider:

a. shall take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
b. shall file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious

**C. Other Obligations**

a. Obligations in respect of REs' engagement or involvement with unregulated entities in the process of wire transfer:
   REs shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned REs shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,
   i) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
   ii) the agreement / arrangement, if any, with such unregulated entities by REs clearly stipulates the obligations under wire transfer instructions; and
   iii) a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.
b. REs' responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities) 56 REs are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, REs shall ensure that they do not process cross-border transactions of designated persons and entities.
c. REs' responsibility to fulfil record management requirements Complete originator and beneficiary information relating to wire transfers shall be preserved by the REs involved in the wire transfer, in accordance with Section 46 of the Master Direction

**80. 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 travellers' 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., This instruction has come into force for such instruments issued on or after September 15, 2018.

**81. Quoting of PAN**

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

**82. Selling Third party products**

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

a. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of the Master Direction of RBI..

b. transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 39.

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

e. transactions involving rupees fifty thousand and above shall be undertaken only by:
   a. debit to customers' account or against cheques; and
   b. obtaining and verifying the PAN given by the account-based as well as walk-in customers.

f. 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 if made available and any other product for rupees fifty thousand and above.

**83. At-par cheque facility availed by co-operative banks**

(a) The 'at par' cheque facility offered to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising there from.

(b) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by bank.

(c) Cooperative Banks shall:

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

ii. maintain the following:
   a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,
   b. sufficient balances/drawing arrangements with the Bank for purpose of honouring such instruments.
   c. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amountinvolved.

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

While issuing the PPI Bank shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

**85. Hiring of Employees and Employee training**

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

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

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

**Annexure 1**

**Digital KYC Process**

a. The Bank shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of the customers and the KYC process shall be undertaken only through this authenticated application,

b. The access of the Application shall be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Bank to its authorized officials.

c. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.

d. The Bank will ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF).Further, the system Application of the Bank shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

e. The Application shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph will be of white colour and no other person will come into the frame while capturing the live photograph of the customer.

f. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

g. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

h. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

i. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may beused for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Bank shall not be used for customer signature. The Bank will ensure that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

j. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Bank. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration.

The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

k. Subsequent to all these activities, the Application shall give information about thecompletion of the process and submission of activation request to activation officer of the Bank, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

l. The authorized officer of the Bank will check and verify that:-

m. information available in the picture of document is matching with the information enteredby authorized officer in CAF.

n. live photograph of the customer matches with the photo available in the document.; and

o. all of the necessary details in CAF including mandatory field are filled properly.;

p. On Successful verification, the CAF shall be digitally signed by authorized officer of the Bank who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

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

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

**Annexure 2**

File No.14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division
North Block, New Delhi

Dated 2nd February, 2021
(Amended vide corrigendum dated March 15, 2023)

**ORDER**

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

1. The Unlawful Activities (Prevention) Act, 1967 (UAPA) was amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51 A, reads as under: -

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

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism:

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism". The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under:-

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

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:
3. Appointment and communication details of the UAPA Nodal Officers:
   3.1 The 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.
   3.3 All the States and UTs shall appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.
   3.4 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all

UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

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

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

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

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

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

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

4.4 The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay. 4.5 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.

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

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

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

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

(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 FIUIND 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):**

(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.
(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/ 67 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. 68

**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; 69

(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 70 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 - 12011/2022-ES Cell-DOR
Government of India
Ministry of Finance
Department of Revenue
***

New Delhi, dated the 30th January, 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"**

I 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;*

*b) 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." 73*

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

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

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

23314459 (FAX), email address: dir@fiuindia.gov.in].

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

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

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all 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') as specified under section 12A (1) to the CNO and Nodal officers.

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

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

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will maintain the designated list and update it, without delay, 74 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.
v. The REs shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 3.1 (i) and (ii) above, carried through or attempted.

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

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

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

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

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

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

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

(j) 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, 77 without delay, and shall freeze any such transaction.

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

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

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

(vii) In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated

individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm, and in case such a request is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

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

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. 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.

5.3. 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.

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

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

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

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

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

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

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

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

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)

| Document Name | KYC AML POLICY | Document Number | OPR/COCI/1.4 |
|---|---|---|---|
| Security Classification | Public | Document Status | |
| Date of Release | June 25, 2023 | Version Number | 1.4 |

**Annexure IV**

**HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/LOCATIONS/ALERTS FOR BRANCHES/ OFFICES**

**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, fund managers, trustees, custodians, etc.

xxi) Trusts, charities, NGOs/NPOs (especially those operating on a ―cross-border‖ basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies).

xxii) Money Service Business: including seller of: Money Orders / Travelers‟ Checks / Money Transmission /Check Cashing / 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.

**2. 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.

## 5. INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES

### A .Countries/Jurisdictions

i) Countries subject to sanctions, embargoes or similar measures in the United Nations
ii) Security Council Resolutions (—UNSCR‖).
iii) Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
iv) Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
v) Tax havens or countries that are known for highly secretive banking and corporate law practices
vi) Countries identified by credible sources as lacking appropriate AML/CFT laws,regulations and other measures.
vii) Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
viii) Countries identified by credible sources as having significant levels of criminal activity.
ix) 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).

**B. 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 continueto show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

**6.INDICATIVE LIST OF SUSPICIOUS CUSTOMER BEHAVIOUR**

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 inthe transaction.

iii. Customers who decline to provide information that in normal circumstances would makethe 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 / debitsis 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

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.

**7. RISK BASED TRANSACTION MONITORING**

**A. Transactions Involving Large Amounts of Cash**

i. Exchanging an unusually large amount of small denomination notes for those ofhigher

denomination

ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlementdespite the customer having an account with the bank.
iii. Frequent withdrawal of large amounts by means of cheques, including traveler's cheques.
iv. Frequent withdrawal of large cash amounts that do not appear to be justified bythe customer's business activity.
v. Large cash withdrawals from a previously dormant/inactive account, or from an accountwhich 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 frequenttransfers 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 thancheques.
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 ofbusinessdoes 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, tohave the report filed or to proceed with a transaction after being informed that the report mustbe 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 a 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 eventhough 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.

E. 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 toprovide 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 bank believes that it would no longer be satisfied that it knows the true identity of theaccount 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 andmoney 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 orbusiness, 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 multiplemonetary 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 travelers 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 arepaid for by multiple Bankers' cheques (just under a specified threshold)

xviii. A Non-customer sends numerous wire transfers using currency amounts just below aspecified threshold limit.

**Annexure V**

**RISK CATEGORISATION**

As per the extant guidelines bank has to devise the procedure for Risk categorization of existing and new customers as per their Risk profiles and to apply various AML measures, keeping in view risk involved ina transaction, account or banking relationship and classify customers into various risk categories i.e. **High Risk, Medium Risk and Low risk** depending on following three parameters: -

A. Country of domicile.
B. Type of product/ service availed.
C. Type of the customer and nature of the business activity.

Apart from above three parameters, the level of Money Laundering Risk that the Bank is exposed to bycustomer relationship also depends upon the Annual income or turn over in the account of the customer. Bank, therefore, has taken into consideration the same as the 4th parameter for categorizing customers into various risk categories.

**Identification of high risk category customer**

- If the country of domicile of the customer falls within the ambit of the high risk category, then the customer is to be classified as high risk category.
- If the activity, nature of business, service etc. of the customer is of high risk category the customer is to be classified as high risk category.
- If the Annual income or turn over depending upon the constitution of the customer fallsunder high risk category the customer is to be classified as high risk category.

**Identification of medium risk category customer**

- If the country of domicile of the customer falls within the ambit of the medium riskcategory, then the customer is to be classified as medium risk category.
- If the activity, nature of business, service etc. of the customer is of medium risk category the customer is to be classified as medium risk category.
- If the Annual income or turn over depending upon the constitution of the customer falls under medium risk category the customer is to be classified as medium risk category.

**Identification of low risk category customer**

Group of all the rest of the accounts which do not fall under high risk or medium risk category shall betreated and classified as low risk category customer.

As Risk Categorization depends upon above said four parameters there are chances that on account ofincrease or decrease of Annual Income or turn over, change in nature of activity and country of residence etc. the risk category may change. Therefore, it is imperative that review of Risk Categorization be carried out biannually in the first seventh calendar month which should be completed by 31st January & 31st July every year.

## 6. Applicability

The policy is effective from June 25, 2023.

## 7. Periodicity of Review of Policy

The policy will be valid upto June 24, 2024. The Approved Policy may be reviewed/ amended before 30.06.2024 if there is any change / fresh guidelines issued by RBI/Government/Bank. The Chairman & CEO may allow continuation of the policy for a maximum period of six months from due date of review, in case the policy cannot be reviewed on or before due date.

**End of Document**