

**KYC STANDARDS AND AML POLICY
(KYC AML CFT POLICY)
OF
THE SOUTH INDIAN BANK LTD**



CONTENTS

Sl no	Particulars
1	Title and commencement
2	Applicable of AML KYC policy
3	Definitions
4	General
5	Key elements of the KYC policy
5A	Money Laundering and Terrorist Financing Risk Assessment by Banks
6	Designated Director
7	Principal Officer
8	Compliance of KYC policy
9	Customer Acceptance Policy.
10	General aspects of customer Acceptance Policy
11	Customer Acceptance Policy for financially or socially disadvantaged customers
12	Risk Management -Risk based approach
13	Customer Identification Procedures
14	Customer Due Diligence (CDD) Procedure- done by a third party
15	Customer Due Diligence (CDD) Procedure in case of Individuals
16	Aadhaar Authentication
17	Video based Customer Identification Process
18	Small Accounts
19	KYC compliance customer account transfer
20	CDD Measures for Sole Proprietary firms
21	Proof of business/ activity in the name of the proprietary
22	Customer point verification
23	CDD Measures for Legal Entities
24	Opening an account of a partnership firm
25	Opening an Account of a Trust
25A	Opening an account of an unincorporated association or a body of individuals
25B	Opening accounts of juridical persons
26	Opening an account of a Legal Person- Identification of Beneficial Owner
27	On-going Due Diligence
28	Close monitoring of certain transactions.
29	Monitoring of transactions based on Risk profile
30	KYC periodic updation
31	Obtaining of Permanent Account Number or equivalent e-document thereof or Form No.60
32	CDD-Non-face to face customer
33	Accounts of Politically Exposed Persons (PEPs)
34	Client accounts opened by professional intermediaries:
35	Simplified norms for Self Help Groups (SHGs)
36	Procedure to be followed by banks while opening accounts of foreign students
37	Simplified KYC norms for Foreign Portfolio Investors (FPIs)
38	Record Management
39	Reporting Requirements to Financial Intelligence Unit – India
40	Reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND.

41	Furnishing information to the Director, FIU- IND
42	Robust software, throwing alerts in case of inconsistent with risk categorization
43	Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967
44	Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)
45	Sanctions List of Designated Individuals and Entities
46	Jurisdictions that do not or insufficiently apply the FATF Recommendations
47	Secrecy Obligations and Sharing of Information:
48	Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010
49	CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)
50	Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)
51	Period for presenting payment instruments
52	Operation of Bank Accounts & Money Mules
53	Collection of Account Payee Cheques
54	Unique Customer Identification Code (UCIC)
55	Introduction of New Technologies.
56	Correspondent Banking
57	Wire transfer
58	Issue and Payment of Demand Drafts, etc.,
59	Quoting of PAN
60	Selling Third party products
61	At-par cheques facility availed by co-operative banks
62	Issuance of Prepaid Payment Instruments (PPIs)
63	Hiring of Employees and Employee training
	Annex-I Digital KYC Process
	Annexure-II -Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.
	Annexure-III - Procedure for implementation of Section 12A of “The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005
64	PFRDA

VERSION

Version	Board approval date	Department
1.0		O & M & Compliance
1.1	10.09.2007	O & M & Compliance
1.2	16.06.2009	O & M & Compliance
1.3	31.08.2010	O & M & Compliance
1.4	27.09.2011	O & M & Compliance
1.5	19.10.2012	O & M & Compliance
1.6	19.04.2013	O & M & Compliance
1.7	19.02.2014	O & M & Compliance
1.8	06.04.2014	O & M & Compliance
1.9	23.05.2015	Compliance
1.10	01.06.2016	Compliance
1.11	11.07.2017	Compliance
1.12	15.10.2018	Compliance
1.13	17.10.2019	Compliance
1.14	27.03.2020	Compliance
1.15	29.06.2020	Compliance
1.16	22.07.2021	Compliance
1.17	30-08-2022	Compliance
1.18	31-05-2023	Compliance
1.19	20-11-2023	Compliance
1.20	21-12-2024	Compliance

Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005

In terms of the Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time. In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

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

Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act *ibid*, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

Banks are also required to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s).

This KYC AML CFT policy has thus been framed in accordance with the regulatory guidelines on KYC (Know Your Customer), AML (Anti Money Laundering), and CFT (Combating of Financing of Terrorism)

1. Title and commencement

Policy is framed in line with RBI Master direction- Know Your Customer (KYC) Direction, 2016 updated as on **November 06, 2024.**

2. Applicability of AML KYC policy

The provisions of these Directions will apply to the branches, subsidiaries and majority owned joint ventures located abroad, to the extent local laws permit of the bank.

Based on this policy, each foreign office of the bank is required to put in place an Anti-Money Laundering Policy (duly approved) which shall also contain the KYC guidelines and Suspicious Activity Reporting (SAR) procedures as may be required by the rules and regulations of the host country provided that

- Where applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of the Reserve Bank of India. RBI may advise further necessary action by the RE including application of additional measures to be taken by the RE to manage the ML/TF risks.
- In case there is a variance in KYC/AML standards prescribed by the Reserve Bank of India and the host country regulators, branches/ subsidiaries of Banks are required to adopt the more stringent regulation of the two.
- Branches, subsidiaries and majority owned joint ventures located abroad may adopt the more stringent regulation of the two i.e. standards prescribed by the Reserve Bank of India and their home country regulators.

Provided that this rule shall not apply to ‘small accounts’ referred to in Serial no :18 of Customer Due Diligence (CDD) Procedure of this policy.

3. Definitions

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

- (a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:
 - i. Bank, at receipt of the Aadhaar number from the customer may carry out authentication of the customer’s Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customer’s declaration that 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) in his account.
 - 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 shareholders agreements or voting agreements.

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

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

- c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals. Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

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

- v. **Certified Copy** - Obtaining a certified copy by the Bank shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the Bank 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:

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

- vi. Central KYC Records Registry” (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- vii. Designated Director" means a person designated by the board to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the Reporting entity is a company. Accordingly, the MD & CEO of the bank is the ‘Designated Director’ of the bank as approved by the Board.
- 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 capturing live photo of (i) the customer and (ii) officially valid document (OVD) or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the bank.
- ix. Digital Signature” shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- x. Equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
- xi. 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 organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).
- xiii. List of Officially Valid Documents (OVD) [any one to be submitted in case of individuals]
- 1) Passport
 - 2) Driving License
 - 3) Proof of possession of Aadhaar number
 - 4) Voter’s Identity Card issued by Election Commission of India
 - 5) Job card issued by NREGA duly signed by an officer of the State Government
 - 6) letter issued by the National Population Register containing details of name and address or any document as notified by RBI / Government in consultation with the regulator.

Provided that

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

b. Proof of Address

In case the OVD furnished by the customer does not contain updated address, the following documents or equivalent e-documents shall be deemed to be OVDs for the limited purpose of proof of address:-

- i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii) property or Municipal tax receipt;
 - iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
- c. Provided further that the customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.
- d. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

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 at the management level nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

- 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 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

- xviii. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in **serial no:18**.

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

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

- xx. Video based Customer Identification Process (V-CIP) is a method of customer identification by an official of the bank, by undertaking seamless, secure, real-time, consent based audio- visual interaction with the customer to obtain identification information including the documents required for customer due diligence (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 Policy.

- xxi. "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).

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

- i. “Common Reporting Standards” (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
- ii. “Customer” means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) i.e., 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 using reliable and independent sources of identification.

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

- a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
 - b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
 - c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.
- 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 USA to 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 to the CKYCR, for individuals and legal entities.
 - ix. “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the Banks or meeting the officials of Banks.
 - x. “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that they are consistent with RE’s knowledge about the customers, customers’ business and risk profile, the source of funds / wealth.

- 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. “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. Asset Reconstruction Companies (ARCs)
 - e. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
 - f. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
- xiv. “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.
- xv. “Wire transfer” means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.
- xvi. “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.
- xvii. Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

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

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

xx. **Wire transfer**

- a. Batch transfer: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.
- b. Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.
- c. Beneficiary Bank: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary Bank and makes the funds available to the beneficiary.
- d. Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
- e. Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.
- f. Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
- g. Financial Institution: In the context of wire-transfer instructions, the term ‘Financial Institution’ shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.
- h. Intermediary Bank: Intermediary Bank refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

- i. **Ordering Bank:** Ordering Bank refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
 - j. **Originator:** Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
 - k. **Serial Payment:** Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).
 - l. **Straight-through Processing:** Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.
 - m. **Unique transaction reference number:** Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
 - n. **Wire transfer:** Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.
- (c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. General

- (a) Know Your Customer (KYC) policy of the bank shall be duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.
- (b) 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). Accordingly this policy may be treated as 'Group-wide KYC AML policy applicable to the bank, its subsidiaries, foreign offices of the bank and forms the base document for implementing group-wide programmes against money laundering and terror financing, for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

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

5. Key element of KYC policy

The KYC policy shall include following four key elements:

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

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

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

The assessment process will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator / supervisor may share with Bank from time to time.

- (b) The risk assessment by the Bank will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/ structure, etc. of the Bank. Further, the periodicity of risk assessment exercise will be determined by Board or any committee of the Board of the bank to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise, which will be reviewed at least annually. Accordingly, as per the decision of Risk Management Committee of the Board (RMCB), ML/TF Risk Assessment of the bank will be carried out for every half year and the same will be approved by RMCB and the same will be placed to Board annually.
- (c) The outcome of the exercise will be put up to Board, and will be available to competent authorities and self-regulating bodies.
- (d) Bank will apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified internally or through national risk assessment) as per the Board approved policies, controls and procedures in this regard. Banks CDD programme will have regard to the ML/TF risks identified and the size of business. Further, bank will monitor the implementation of the controls and enhance them if necessary.

6. Designated Director:

- (a) A “Designated Director” means a person designated by the Bank to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.
- (b) Board has approved MD & CEO of the bank as the Designated Director for PMLA and as and when there is a change in the MD& CEO of the bank, the same shall be duly communicated to FIU-IND.

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

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

7. Principal Officer:

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

8. Compliance of KYC policy

- (a) Bank will ensure compliance with KYC Policy through:
 - i. Specifying as to who constitute ‘Senior Management’ for the purpose of KYC compliance. Bank has fixed Scale V and above officers of the bank as ‘Senior Management’ for the purpose of KYC compliance.
 - ii. Allocation of responsibility for effective implementation of policies and procedures.
 - iii. Submission of quarterly audit notes and compliance to the Audit Committee.
- (b) Bank to ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
- (c) Compliance Function
 - i. Evaluating and ensuring adherence to the KYC policies and procedures (based on KYC Inspection reports, feedback from CPC etc) by the branches.
 - ii. Independent evaluation of the bank’s own KYC/AML/CFT policies and procedures vis-à-vis legal and regulatory requirements.

(d) Risk Management

The Board of Directors of the bank is responsible and committed to ensure that an effective KYC programme is put in place in the bank by establishing appropriate procedures and to ensure their effective implementation to achieve full compliance of KYC/AML/CFT guidelines of RBI in letter and spirit.

(e) The Machinery for implementing the KYC Programme consists of:

i. Board of Directors

- a. Tasked with Formulating appropriate KYC/AML policies from time to time
- b. Direction and Advise on compliance of KYC/AML/CFT guidelines

ii. Audit Committee of the Board

Tasked with:

- a. the oversight of KYC/AML Compliance
- b. Review of KYC Inspection reports and status of rectification
- c. Identifying compliance threats

iii. Designated Director (MD&CEO)

Ensures overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include Oversight of implementation of the policies formulated by the Board Liaisoning with Director FIU-IND.

iv. AML Principal Officer (MLRO)

- a. Monitoring the implementation of the bank's KYC/AML policy.
- b. Maintaining liaison with law enforcement agencies ensuring submission of periodical Reports to the top Management/board.
- c. Oversight of timely submission of reports to FIU-IND viz., CTR, STR, CCR,NTR, Cross Border Wire transfers >5 lacs etc
- d. Formulation of Proper systems, procedures and Controls in the KYC/AML area
- e. Devise procedures for creating risk profiles of their existing and new customers
- f. Assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc
- g. Staff Training Programme on KYC/AML guidelines

v. Central AML Cell

- a. Transaction Monitoring through AML application
- b. Maintenance and development/ customization of AML application in liaison with DICT and the system Vendor
- c. Timely submission of reports to FIU-IND viz., CTR, STR, CCR, NTR, Cross Border Wire transfers > 5 lacs etc.
- d. KYC/AML Inspection Reports
- e. Train the staff on KYC/AML guidelines

vi. Inspection & Vigilance Department

Conducting Regular, Concurrent and Special KYC audits and to verify compliance with KYC/AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee.

vii. Regional Offices:

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

viii. Centralized Processing Centre

The Bank have implemented Centralized Processing Center (CPC) Model for on boarding new customers in all regions.

9. Customer Acceptance Policy

The Bank will accept customers after verifying their identity as laid down in Customer Identification Procedures detailed under Customer Identification Procedure (CIP) serial no.13 of this Policy. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and PML rules, 2005 , and instructions/guidelines issued by Reserve Bank from time to time.

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

- (a) The Bank will not open accounts in the name of anonymous / fictitious / benami persons/ names.
- (b) The Bank will not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the bank. The decision by a branch to close an account in such cases should be taken by the Regional Office of the branch and the Branch shall close the account only after giving due notice to the customer explaining the reasons for such a decision. Regional office if finds any kind of suspicious activity under such situations, should inform the same to Compliance department and sanction for closure of account should be provided only after concurrence from Compliance department. Bank if finds any kind of suspicious activity under such situations shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer. If bank decides to file STR, such accounts shall not be closed to avoid tipping of STR.
- (c) No transaction or account based relationship is to be undertaken without following the Customer Due Diligence (CDD) procedure.
- (d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, as specified.
- (e) Additional information required by the bank, is obtained with the explicit consent of the customer. All the mandatory as well as additional information required by the bank is specified in the SOP of the Centralized Processing Centre of the bank through which customers are on-boarded and updated as and when required.
- (f) The Bank will apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of a Bank desires to open another account **or avail any other product or service** with the same Bank, there shall be no need for a fresh CDD exercise **as far as identification of the customer is concerned.**

- (g) CDD Procedure is followed for all the joint account holders, while opening a joint account.
- (h) In occasions when an account is requested to be operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity, the Bank will enquire and ascertain the circumstances, in which a customer is permitted to act on behalf of another person/entity and will be clearly spelt out in conformity with the established law and practice of banking.
- (i) The Bank will do necessary checks before opening a new account, by way of a search of UN list of terrorists published by RBI and by way of a search in other public domain, if required, so as to ensure 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. (Sanctions lists indicated in serial no 43 of the KYC AML CFT POLICY.)
- (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 to verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- (l) Where Goods and Services Tax (GST) details are available, the GST number will be verified from the search/verification facility of the issuing authority.

11. Customer Acceptance Policy in case of financially or socially disadvantaged

Customer Acceptance Policy shall not strive to inconvenience the general public, especially those who are financially or socially disadvantaged. In order to avoid disproportionate cost to the banks and a burdensome regime for the customers, a risk based approach to be followed in the KYC Guidelines issued.

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

Risk Management

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

- (a) The customers will be risk categorized based on the assessment and risk perception of the bank as follows:
 - i. Low Risk
 - ii. Medium Risk
 - iii. High Risk

Risk categorization of each customer into low, medium and high risk category based on the assessment and risk perception of the customers and not merely based on any group or class they belong to.
- (b) Broad principles may be laid down by the Bank for risk-categorisation of customers.
- (c) Risk categorization will be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- (d) **The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.**

Bank will ensure that the information sought from the customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued. Bank may seek any other optional/ additional information from the customer separately, after opening the account and with the explicit consent of the customer only.

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

13. Customer Identification Procedure (CIP)

Bank undertake identification of customers in the following cases:

- (a) While establishing a banking relationship i.e., an account based relationship.
- (b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.
- (c) When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
- (d) Selling third party products as agents, selling their 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 a Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold

of rupees fifty thousand

(g) Introduction shall not be sought while opening accounts.

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Banks, shall at their 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 immediately from the third party or from the Central KYC Records Registry.
- (b) Adequate steps are taken by banks 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.
- (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.

Customer Due Diligence (CDD) Procedure

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

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

- (a) the Aadhaar number where,
 - i. Bank shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - ii. he decides to submit his Aadhaar number voluntarily to a bank or any Bank notified under first proviso to sub-section (1) of section 11A of the PML Act; or
- aa the proof of possession of Aadhaar number where offline verification can be carried out; or
- ab the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document there of 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 in Income-tax Rules, 1962; and
- (c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Bank:

Provided that where the customer has submitted,

- i. Aadhaar number under clause (a) above to a bank or to a Bank notified under first provision to sub-section (1) of section 11A of the PML Act, such bank or Bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.
- ii. proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.
- iii. an equivalent e-document of any OVD, the Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.
- iv. any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Bank shall carry out verification through digital KYC as specified under Annex I.
- v. KYC Identifier under clause (ac), Bank shall retrieve the KYC records online from the CKYCR in accordance with serial no :49 as specified under this policy

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 pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD 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 serial no 8(e)(vi) under this 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 its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

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

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act 2016, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

16. Aadhaar Authentication

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

- (a) There must be a specific consent from the customer for authentication through OTP.
- (b) 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 (e) below is complete.
- (c) the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- (d) 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.
- (e) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which biometric based Customer Due Diligence as per serial no 15 or as per serial no:17 (V-CIP). If Aadhaar details are used under serial no:17, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- (f) If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
- (g) 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 indicate that such accounts are opened using OTP based e-KYC and other banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.
- (h) 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
- (i) As a risk-mitigating measure for such accounts, bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar.

17. Video based Customer Identification Process (V-CIP)

Bank may undertake live V-CIP, to be carried out by an official of the bank, for:

- i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, bank shall also obtain the equivalent e-document of the activity proofs as mentioned in serial no 21 and serial no 22 with respect to the proprietorship firm, apart from undertaking CDD of the proprietor.
- ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per serial no 16 of this policy.
- iii. Updation/ Periodic updation of KYC for eligible customers.

(a) V-CIP Infrastructure

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

- i. Bank should have complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in

own premises of the Bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. Bank shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure shall be housed in own premises of the bank and the V-CIP connection and interaction shall necessarily originate from own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Bank.

- ii. Bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.
- iii. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iv. The video recordings should contain the live GPS co-ordinates (geo- tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- v. Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cybersecurity event under extant regulatory guidelines.
- vi. The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
- vii. The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines

(b) V-CIP Procedure

- i) Bank shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Bank specially trained for this purpose. The official should be capable to carry out

liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

- ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Bank. However, in case of call drop / disconnection, fresh session shall be initiated.
- iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.
- iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.
- v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.
- vi) The authorized official of the bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
 - a. OTP based Aadhaar e-KYC authentication.
 - b. Offline Verification of Aadhaar for identification.
 - c. KYC records downloaded from CKYCR, in accordance with serial no: 49, using the KYC identifier provided by the customer.
 - d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

Bank shall ensure to redact or blackout the Aadhaar number in terms of serial no: 15 mentioned under this policy.

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 working days from the date of carrying out V-CIP.

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

- vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
- viii) Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.
- ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
- x) The authorized official of the bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and

the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

- xi) Assisted V-CIP shall be permissible when banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.
- xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.
- xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank

(c) V-CIP Records and Data Management

- i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in Policy on Preservation of old records policy of the bank, shall also be applicable for V-CIP.
- ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

18. Small Accounts:

Notwithstanding anything contained in serial no:15 of this policy 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:

A Small account is one where all the following conditions are met:

- i) The aggregate of all credits in a financial year does not exceed Rs.1.00 lakh;
- ii) The aggregate of withdrawals and transfers in a month does not exceed Rs.10,000/-.
- iii) The balance at any point of time does not exceed Rs.50,000/-.

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

Further, small accounts are subject to the following conditions:

- a. The bank shall obtain a self-attested photograph from the customer.
- b. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
- c. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
- d. Banks shall ensure that the stipulated monthly and annual limits on aggregate of

transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.

- e. The account remains operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
- f. The entire relaxation provisions shall be reviewed after twenty four month.
The account remains 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. Notwithstanding anything contained in clauses (e) and (f) above, the small account period shall remain operational as may be notified by the Central Government.
- h. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of “officially valid documents” as referred in the List of Officially Valid Documents and the Aadhaar number of the client or where an Aadhaar number has not been assigned to the client, through the production of proof of application towards enrolment for Aadhaar along with an officially valid document.
Provided further that if the customer is not eligible to be enrolled for an Aadhaar number, the identity of the customer shall be established through the production of an officially valid document as per serial no:15 or Serial no:17 mentioned in this policy.
- i. Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of “officially valid documents” as referred in the List of Officially Valid Documents and the Aadhaar number of the client or where an Aadhaar number has not been assigned to the client, through the production of proof of application towards enrolment for Aadhaar along with an officially valid document. Provided further that if the customer is not eligible to be enrolled for an Aadhaar number, the identity of the customer shall be established through the production of an officially valid document as per serial no:15 or Serial no:17 mentioned in this policy.

19. KYC compliance customer account transfer

If an existing KYC compliant customer of a branch desires to open another account with the same bank, there shall be no need for a fresh CDD exercise. KYC exercise once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account and the same is not due for periodic updation and a self-declaration from the account holder about his/her current address is obtained in such cases. The customer should be allowed to transfer his account from one branch to another branch without restrictions.

20. CDD Measures for Sole Proprietary firms

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

21. Proof of business/ activity in the name of the proprietary

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

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

22. Customer point verification

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

CDD Measures for Legal Entities

23. Opening an account of a Company

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

- a. Certificate of incorporation
- b. Memorandum and Articles of Association
- c. Permanent Account Number of the company
- d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
- e. Customer Due Diligence and KYC documents of the individuals (Directors, Beneficial owners, Managers/Officers/Employees holding an attorney to transact on the company's behalf if any)
- f. The names of the relevant persons holding senior management position; and
- g. The registered office and the principal place of its business, if it is different.

Branches should not generally insist on affixing of Company Seal in Memorandum and Articles of Association while opening account of a Company. However, Branches should insist on affixing of Company Seal in Memorandum and Articles of Association/other specified documents, while opening account of a Company, when the requirement of affixing of Company Seal is specifically mentioned in Memorandum or Articles of Association, of the Company.

24. Opening an account of a Partnership firm

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

- a. Registration certificate
- b. Partnership deed
- c. Permanent Account Number of the partnership firm
- d. Customer Due Diligence and KYC documents of the individuals (Partners, Beneficial owners, person holding an attorney to transact on its behalf if any).
- e. The names of all the partners and
- f. Address of the registered office, and the principal place of its business, if it is different.

25. Opening an Account of a Trust

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

- a. Registration certificate
- b. Trust deed
- c. Permanent Account Number or Form No.60 of the trust
- d. Customer Due Diligence and KYC documents of the individuals (Trustees, Beneficial owners, person holding an attorney to transact on its behalf if any)
- e. The names of the beneficiaries, trustees, settlor, **protector, if any** and authors of the trust.
- f. The address of the registered office of the trust; and
- g. List of trustees and documents, as specified in Serial no 15, for those discharging the role as trustee and authorized to transact on behalf of the trust.

25A. Opening an account of an Unincorporated association or a body of individuals

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

- a. Resolution of the managing body of such association or body of individuals.
- b. Permanent Account Number or Form No. 60 of the unincorporated association or body of individuals.
- c. Power of attorney granted to transact on its behalf
- d. Customer Due Diligence and KYC documents of the individuals (including beneficial owners, person holding an attorney to transact on its behalf if any).
- e. Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trust/ partnership firms shall be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies

25B. Opening Accounts of Juridical Persons

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

- a. Document showing name of the person authorized to act on behalf of the entity;
- b. Documents, as specified in serial no:15, 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.

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

26. Opening an account of a Legal Person- Identification of Beneficial Owner

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 (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- b. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

27. On-going Due Diligence

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

28. Close monitoring of certain transactions.

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.

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

29. Monitoring of transactions based on Risk profile

Monitoring of transactions will be conducted taking into consideration the risk profile of the account.

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

- a. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and enhanced due diligence measures are put in place.
- b. Branches have to take due care while opening accounts of Multi-Level Marketing agencies to ensure that the firms are not being engaged in deposit taking activities and the funds raised by them are not being used for any illegal activities. Branches should closely monitor the transactions in accounts of marketing firms.

In 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, the branches should carefully analyse such data and in case they find such unusual operations in accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance, through Compliance department.

30. Updation / Periodic Updation of KYC

Periodic updation from the date of opening of the account / last KYC 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 for ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk as per the following procedure:

(a) Individual customers:

- i. No change in KYC information: In case of no change in the KYC information, a

self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application), letter etc.

In case of a change only in the address details of the customer, as per RBI regulation, customers have the option to submit a self- declaration of the new address through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter etc., in which case the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

- ii. However, considering the risk involved in accepting such declaration without proper proof of address, Bank may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in serial no: 3(a)(xiii) of this policy, for the purpose of proof of address, declared by the customer at the time of **updation**/periodic updation as per the provision provided to bank in the RBI regulation.
- 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 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.
- iv. Aadhaar OTP based e-KYC in non-face to face mode may be used for **updation** /periodic updation. To clarify, conditions stipulated in Serial no 16 in this policy 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. Banks shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

(b) Customers other than individuals:

- i. No change in KYC information: In case of no change in the KYC information of the Legal entity (LE) customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter from an official authorized by the LE in this regard, board resolution etc. Further, 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.
- ii. 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 LE customer.

(c) 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 branches are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the branches 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 details, if available with the branches, is 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 **updation**/periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of **updation** /periodic updation of KYC are promptly updated in the records / database of the bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- iv. In order to ensure customer convenience, Bank may consider making available the facility of **updation** /periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Bank or any committee of the Board to which power has been delegated.
- v. Bank shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Bank such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly approved by the Board of Directors of reporting entity or any committee of the Board to which power has been delegated.

(d) 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 Bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank end.

31. Obtaining of Permanent Account Number or equivalent e-document thereof or Form No.60

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-document thereof or Form No. 60 is submitted by the customer.

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

provide appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

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

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

Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

32. CDD- Non-face to face customer

Enhanced Due Diligence (EDD) for non-face-to-face customer on boarding (other than customer on boarding in terms of Serial no 16 mentioned in this policy i.e., Accounts opened using Aadhaar OTP based e-KYC), in Non-face-to-face on boarding facilitates the Bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, 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 Bank for non-face-to-face customer on boarding (other than customer on boarding in terms of Serial no: 16):

- (a) In case Bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this KYC AML CFT POLICY.
- (b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Change of mobile number and email id will be allowed only after the identity of the customer is verified in face-to-face manner or through V-CIP.
- (c) Apart from obtaining the current address proof, Bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- (d) Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- (e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
- (f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

33. Accounts of Politically Exposed Persons (PEPs)

Bank identifies PEP by verifying the details of every Customer or Beneficial Owner being on-boarded as well as reviews existing customer with the PAP database available in Rifinitiv application integrated with customer on-boarding platform of the bank. Identified PEP are subjected to following enhanced due diligence process:

- (a) Branches should verify the identity of the person and seek information about the sources of funds of family members and close relatives is gathered before accepting the PEP as a customer
- (b) Branches should gather sufficient information and Identity of a person/customer of this category intending to establish a relationship and also check all the information available on the person in the public domain
- (c) Branches should also subject such accounts to enhanced monitoring on an ongoing basis
- (d) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, branches should obtain Regional Head approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.
- (e) Branches should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

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

Explanation: For the purpose of this section, “Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

PEP in case of beneficial owner

The above instructions shall also be applicable to accounts where a PEP is the beneficial owner.

34. Client accounts opened by professional intermediaries

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

- (a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
- (b) Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
- (c) Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
- (d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the Bank shall look for the beneficial owners.
- (e) Bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
- (f) The ultimate responsibility for knowing the customer lies with the Bank.

B. Simplified Due Diligence

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

36. Accounts of Foreign Students

- (a) Branches shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
 - 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 Reserve Bank 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 the account.

37. 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 of (Master direction- Know Your Customer (KYC) Direction, 2016 updated as on November 06, 2024)** 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.

38. Record Management

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

- (a) In terms of PML Amendment Act 2012 notified on February 15, 2013, banks should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

- (b) Branches should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.
- (c) Such records and related documents will be made available swiftly to auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities, on demand.
- (d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005).
- (e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
 - i. the nature of the transactions;
 - ii. the amount of the transaction and the currency in which it was denominated;
 - iii. the date on which the transaction was conducted; and
 - iv. the parties to the transaction.
- (f) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities
- (g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

- 38A. 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. 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.

39. Reporting Requirements to Financial Intelligence Unit – India

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

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

40. Reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND.

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 Report (CTR)/ Suspicious Transaction Report (STR) which FIU-IND has placed on its website shall be made use of by banks for extracting CTR/STR from their live transaction data. The Principal Officers 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 help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website <http://fiuind.gov.in>.

41. Furnishing information to the Director, FIU- IND

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 constitutes as a separate violation. Bank shall not put any restriction on operation in the accounts merely on the basis of the STR filed. Bank, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of this policy of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

42. Robust software, throwing alerts in case of inconsistent with risk categorization

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.

Requirements /obligations under International Agreements Communications from International Agencies

43. 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”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at <https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl>
 - ii. The “1988 Sanctions List”, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at <https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl>.

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

(b) Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND

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 as mentioned in (Annex II of Master direction- Know Your Customer (KYC) Direction, 2016 dated 10th May 2021)

(c) Freezing of Assets under Section 51A of UAPA -Unlawful Activities (Prevention) (UAPA)

Freezing of Assets under Section 51A of UAPA, 1967 -The Bank will strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 as mentioned in (Annex: II) of Master direction- Know Your Customer (KYC) Direction, 2016 dated 10th May 2021)) and ensure meticulous compliance to the Order issued by the Government. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

44. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):which read as follows

- (a) Bank shall ensure meticulous compliance with the “Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005” laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annex III as enclosed of this circular).
- (b) In accordance with paragraph 3 of the aforementioned Order, Bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.
- (c) Further, Bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.
- (d) In case of match in the above cases, Bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Bank

shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

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

- (e) Bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.
- (f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Bank shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.
- (g) In case an order to freeze assets under Section 12A is received by the Bank from the CNO, Bank shall, without delay, take necessary action to comply with the Order.
- (h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Bank 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.

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

45A. Bank shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

45B. Bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organization of which India is a member and accepted by the Central Government.

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

- (a) The Bank will take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, the bank will also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. Bank shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

- (b) The Bank will give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in serial no:46(a) and (b) do not preclude Banks 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.

47. 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 any other purpose without the express permission of the customer.
- (c) While considering the requests for data/information from Government and other agencies, bank shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
- (d) The exceptions to the said rule shall be where:
 - i. disclosure is under compulsion of law
 - ii. where there is a duty to the public to disclose,
 - iii. **Where** the interest of bank requires disclosure
 - iv. where the disclosure is made with the express or implied consent of the customer.

48. Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

Banks shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, banks shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

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

- (a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- (b) In terms of provision of Rule 9(1A) of PML Rules, the Bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

- (c) Operational Guidelines for uploading the KYC data have been released by CERSAI.
- (d) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- (e) Bank is required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR.
- (f) Bank shall upload KYC records pertaining to accounts of Legal Entities (LE) opened on or after April 1, 2021, with CKYCR. The KYC records have to be uploaded as per the LE Template released by CERSAI.
- (g) Once KYC Identifier is generated by CKYCR, bank shall ensure that the same is communicated to the individual/LE as the case may be.
- (h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per clause (e) and (f) respectively at the time of periodic updation as specified in serial no:30 of this policy, or earlier, when the updated KYC information is obtained/received from the customer.

Also, whenever the Bank obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an Bank regarding an update in the KYC record of an existing customer, the Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank.

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

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

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

- (a) Register on the related e-filing portal of Income Tax Department as Reporting Financial Institution.
- (b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at <http://www.fedai.org.in/RevaluationRates.aspx> for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

- (c) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
- (d) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
- (e) 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>.

51. Period for presenting payment instruments

Bank will not make payment of cheques /drafts/banker's cheques, if they are presented beyond the period of three months from the date of such instrument, w.e.f 01/04/2012

52. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the branch has not complied with these directions.

53. Collection of Account Payee Cheques and At-par cheques facility

Account payee cheques for any person other than the payee constituent shall not be collected. Branch shall, at their option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies, and after getting approval for the arrangement from Regional office, and executing necessary document / agreement for the arrangement.

54. Unique Customer Identification Code (UCIC)

- (a) Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by banks.
- (b) The branches shall, at their 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.

55. Introduction of New Technologies

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

Further, Bank shall ensure:

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

56. Correspondent Banking

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

- (a) Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.
- (b) The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.
- (c) Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.
- (d) Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.
- (e) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.
- (f) The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.
- (g) We will ensure that we do not enter into any relationships with 'shell banks' and before establishing any correspondent banking relationship with any foreign institution, branches should take appropriate measures to satisfy themselves.

- (h) It shall be ensured that foreign correspondent institution does not permit its accounts to be used by shell banks. A shell bank is a financial institution which does not have any physical presence in any country.
- (i) Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
- (j) Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

57. Cross-border wire transfers:

A. Information requirements for wire transfers for the purpose of this AML KYC and CFT policy:

- i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:
 - 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 Bank, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.
- iv. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering Bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers. In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering Bank and where the information accompanying the wire transfer can be made available to the beneficiary bank and appropriate authorities by other means, it is sufficient for the ordering Bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering Bank shall make the information available within three working/business days of receiving the request from the intermediary bank, beneficiary bank, or from appropriate competent authorities.
- v. Bank shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement 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 Bank to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

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

i. Ordering Bank:

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

ii. Intermediary Bank

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

appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iii. Beneficiary Bank:

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

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

i. Obligations in respect of Bank engagement or involvement with unregulated entities in the process of wire transfer.

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

- a) there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
- b) the agreement / arrangement, if any, with such unregulated entities by Bank clearly stipulates the obligations under wire transfer instructions; and
- c) a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

ii. Bank responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)

Bank are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with serial no 43 Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967 of the AML KYC and CFT policy, Bank shall ensure that they do not process cross-border transactions of designated persons and entities.

iii. Bank responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the Bank involved in the wire transfer, in accordance with serial no. 38 of this policy.

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

Any remittance of funds by way of demand draft, mail/ telegraphic transfer/ NEFT/ IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment. Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheques, etc. issued by the Bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

59. 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.

60. Selling Third party products

Bank acting as agents 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 this Policy**.
- (b) Transaction details of sale of third party products and related records shall be maintained as prescribed in serial no: 38.
- (c) AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
- (d) transactions involving rupees fifty thousand and above shall be undertaken only by:
 - debit to customers' account or against cheques; and
 - Obtaining and verifying the PAN given by the account-based as well as walk-in customers.
- (a) Instruction at 'd' above shall also apply to sale of Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

61. At-par cheques facility availed by co-operative banks:

- (a) The 'at par' cheques facility offered by commercial banks 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. Approval for such arrangement shall be obtained from Regional office, and necessary document/ agreement for the arrangement executed.
- (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 banks.
- (c) Cooperative Banks shall:
 - i. ensure that the 'at par' cheques facility is utilized only:
 - a. for their own use,
 - b. for their account-holders who are KYC compliant, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
 - c. for walk-in customers against cash for less than rupees fifty thousand per individual.
 - ii. maintain the following:
 - a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheques,
 - b. Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honoring such instruments.
 - iii. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

62. Issuance of Prepaid Payment Instruments (PPIs):

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

63. Employees' Training/Employees' Hiring

- (a) Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
- (b) Bank shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.
- (c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of

customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Bank, regulation and related issues shall be ensured.

64. Pension Fund Regulatory and Development Authority(PFRDA)

PFRDA account will be opened by accepting KYC documents as detailed in Annexure B of this policy which is been framed in line with PFRDA regulatory guidelines on KYC (Know Your Customer), AML (Anti Money Laundering), and CFT (Combating of Financing of Terrorism) Updated as on 23-09-2024.

Annex I

Digital KYC Process

- A. Bank shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of customers and the KYC process shall be undertaken only through this authenticated application of the bank.
- B. The access of the Application shall be controlled by the bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the bank to its authorized officials.
- C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the bank or vice-versa. The original OVD shall be in possession of the customer.
- D. The bank must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF) / Account Opening Form (AOF). Further, the system Application of the bank shall put a water-mark in readable form having CAF/AOF number, GPS coordinates, authorized official's name, unique employee Code (assigned by bank e.g. PPC) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- E. The Application of the bank shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
- G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
- H. Thereafter, all the entries in the CAF/AOF 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 manually filling 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/AOF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF/AOF. In any case, the mobile number of authorized officer registered with the bank shall not be used for customer signature. Bank must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
- J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized

official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the bank. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

- K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the bank, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference- id number to customer for future reference.
- L. The authorized officer of the bank shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF/AOF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF/AOF including mandatory field are filled properly.;
- M. On Successful verification, the CAF/AOF shall be digitally signed by authorized officer of the bank who will take a print of CAF/AOF, 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.

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

Annex II

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

Dated: the 2nd February, 2021

ORDER

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

1. Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) reads as under:-
"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —
 - a. freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
 - b. prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
 - c. prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

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

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:
3. Appointment and communication details of the UAPA Nodal Officers:
 - 3.1. The **Joint Secretary** (CTCR) Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA [Telephone Number: 011-23093124, 011-230923465 (Fax), email address: jsctcr-mha@gov.in].
 - 3.2. The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.
 - 3.3. 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 FIU-IND covering all transactions in the accounts, covered under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.
- 5.2. On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/ entities identified by the banks, stock exchanges/depositories, intermediaries and insurance companies are the ones listed as designated individuals/ entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.
- 5.3. In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The Central [designated] Nodal Officer for the UAPA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.
- The order shall be issued without prior notice to the designated individual/entity.

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

- 6.1. The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable

properties in their respective jurisdiction, without delay.

- 6.2. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.
- 6.3. The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.
- 6.4. The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.
- 6.5. In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.
The order shall be issued without prior notice to the designated individual/entity.
- 6.6. Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

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

- i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.
- ii) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.
- iii) 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.

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

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

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

- 8.1. The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.
 - 8.2. To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.
 - 8.3. The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND and to the Nodal Officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.
9. Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed.
- The freezing orders shall be issued without prior notice to the designated persons involved.

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

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

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

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

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

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

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

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

10.3. .

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

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

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

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

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

11.3. The Central [designated] Nodal Officer for the UAPA shall cause such verification, as

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

- 11.4. 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 1st September, 2023

ORDER

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

- (1) 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.”

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, 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 sub-section (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post, without delay.
- 4.2. the State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.
- 4.3. The State Nodal Officer may cause such inquiry to be conducted by the State Police so

as to ensure that the particulars sent are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed, within 24 hours of the verification, if it matches, with the particulars of the designated individual/entity, to the CNO without delay by email, FAX and by post.

- 4.4. The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.
 - 4.5. In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All Nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals / entities. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.
 - 4.6. The order shall be issued without prior notice to the designated individual/entity.
5. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs):
- i. The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Nodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.
 - ii. Registrar of Societies/ Firms/ non-profit organizations are required to ensure that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure that no societies/ firms/ non-profit organizations should be allowed to be registered if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and, in case, such request is received, then the Registrar shall inform the State Nodal Officer, without delay
 - iii. The State Nodal Officer shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or

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

- iv. The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI), requesting them to sensitize their respective members to the provisions of Section 12A, so that, if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.
 - v. The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs.
 - vi. In addition, a member of the ICSI shall, if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.
 - vii. In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm, and in case such a request is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.
 - viii. All communications to Nodal officer as enunciated in 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

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)

Annexure B

**KYC/AML/CFT Policy of the Bank as POP (Point of Presence) of PFRDA
(Pension Fund Regulatory and Development Authority)**

(Version 1.1)

CONTENTS

Sl no	Particulars
1.	Introduction
2.	Money Laundering
3.	Definitions
4.	Internal policies, procedures, controls, responsibility and compliance arrangement
5.	Appointment of a Designated Director and a Principal Officer
6.	Recruitment and Training
7.	Internal Control/Audit
8.	Know Your Customer (KYC) Norms
9.	Risk Assessment and Risk Categorization
10.	Simplified Due Diligence (SDD)
11.	Enhanced Due Diligence (EDD)
12.	Sharing KYC information with Central KYC Registry (CKYCR)
13.	Reliance on third party KYC
14.	Pension accounts of Politically Exposed Persons (PEPs)
15.	Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)
16.	Prospects residing in the jurisdiction of countries identified as deficient in AML/CFT regime
17.	Reporting Obligations
18.	Record Keeping
19.	Monitoring of Transactions
	Annexure 1- Certificate of Compliance with respect to KYC/AML/CFT
	Annexure 2- Circular ref no. PFRDA/2020/46/SUP-CRA/18 dated 06.10.2020 on Video based Customer Identification Process (VCIP) for NPS
	Annexure 3- Circular ref no. PFRDA/2021/5/PDES/5 dated 03.02.2021 on Digilocker for National Pension System Services.
	Annexure 4- Circular ref no. PFRDA/2019/16/PDES/2 dated 23.09.2019 on Utilization of SEBI KRAs by PoPs for on-boarding of subscriber in NPS

VERSION

Version	Board approval date	Department
1.0	27.03.2024	Compliance Department
1.1	21-12-2024	Compliance Department

1. Introduction

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

Pension Fund Regulatory and Development Authority (PFRDA) issued guidelines on Know Your Customer/Anti- Money Laundering/Combating the Financing of Terrorism (KYC/AML/CFT) by exercising the power conferred under Section 14(1) of Pension Fund Regulatory and Development Authority Act, 2013(PFRDA Act) and provisions 4,5,7,9, 9A & 10 of the PML Rules.

NPS has an unbundled Architecture, where each function is performed by different intermediaries appointed by the PFRDA viz. Pension Funds, Custodian, Central Recordkeeping Agency (CRA), National Pension System Trust, Trustee Bank, Points of Presence (PoP), **Retirement Advisers (RAs)** and Annuity Service Providers (ASPs). Wherein, the role of CRA is recordkeeping, administration and customer service functions for all the subscribers of the NPS including issuance of unique Permanent Retirement Account Number (PRAN) to each subscriber, maintaining a database of all PRANs issued and recording transactions relating to each subscriber's PRAN.

2. Money Laundering

Money Laundering is a process or activity through which proceeds of crime (i.e., illegally acquired money) are converted in the financial systems (by means of undertaking transactions) so that it appears to be legally acquired. Section 3 of PML Act specifies the Offence of Money Laundering.

In terms of the provisions of Prevention of Money Laundering Act, 2002 (PML Act) and the Prevention of Money Laundering (Maintenance of records) Rules, 2005 (PML Rules), Banks are required to follow Customer Identification Procedures (CIP) while undertaking a transaction at the time of establishing an account-based relationship/client-based relationship and monitor their transactions on an on-going basis.

The obligation to establish an anti-money laundering mechanism and formulate and implement a Client Due Diligence (CDD) Programme applies to Banks as per provisions of clause (ii) and (iii) sub rule (14) of Rule 9 of the PML Rules. Bank shall have the responsibility for guarding against NPS, NPS Lite, APY or any other pension scheme regulated / administered by PFRDA being used to launder unlawfully derived funds or to finance terrorist acts. Banks shall take steps to implement provisions of the PML Act and the PML Rules, as amended from time to

time, including operational instructions issued through circulars/guidelines/directions in pursuance of such amendment(s).

3. Definitions

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

3.1 “Aadhaar number”, shall have the meaning assigned to it under clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter referred to as “Aadhaar Act”.

3.2 “Act / PML Act / PMLA” means the Prevention of Money Laundering Act, 2002.

3.3 “Authentication”, means the process as defined under clause (c) of section 2 of the Aadhaar Act.

3.4 “Central KYC Records Registry” (CKYCR) means an entity defined under clause (ac) of sub rule (1) of Rule 2 of the PML Rules.

3.5 “Certified copy” shall mean comparing the copy of officially valid document so produced by the subscriber with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by PFRDA.

3.6 “Client” shall have the meaning assigned to it under clause (ha) of sub section (1) of Section 2 of the PML Act.

3.7 “Client Due Diligence” (CDD) shall have the meaning assigned to it under clause (b) of sub-rule (1) of Rule 2 of the PML Rules.

3.8 “Designated Director” shall have the meaning assigned to it under clause (ba) of sub- rule (1) of Rule 2 of the PML Rules.

3.9 “Digital KYC” shall have the meaning assigned to it under clause (bba) of sub-rule (1) of Rule 2 of the PML Rules.

3.10 “Equivalent e-document” shall have the meaning assigned to it under clause (cb) of sub-rule (1) of Rule 2 of the PML Rules.

3.11 “Financial Group” means a group that consists of a parent company or of any other type of entity exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

3.12 “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR.

3.13 “KYC Identifier” shall have the meaning assigned to it under clause (cc) of sub rule (1) of Rule 2 of the PML Rules.

3.14 “KYC Records” shall have the meaning assigned to it under clause (cd) of sub-rule (1) of Rule 2 of the PML Rules.

3.15 “Non-face-to-face customers” shall have the same meaning assigned to it under sub clause (ix) of 3(b) of Chapter I of Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.

3.16 “Offline verification” shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act.

3.17 “On-going Due Diligence” means regular monitoring of transactions to ensure that they are consistent with the subscriber’s profile and source of funds.

3.18 "Officially valid document" shall have the meaning assigned to it under clause (d) of sub-rule (1) of Rule 2 of the PML Rules.

3.19 "Politically Exposed Persons" (PEPs) shall have the same meaning assigned to it under sub clause (xii) of 3(b) of Chapter I of Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.

3.20 "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 PFRDA.

3.21 "Principal Officer" shall have the same meaning assigned to it under clause (f) of sub-rule (1) of Rule 2 of the PML Rules.

3.22 "Reporting entity" has the same meaning assigned to it under clause (wa) of sub section (1) of section 2 of the PML Act.

3.23 "Rules / PML Rules" means the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

3.24 "Suspicious Transaction" shall have the meaning assigned to it under clause (g) of sub-rule (1) of Rule 2 of the PML Rules.

3.25 "Video Based Customer Identification Process (VCIP)" means an alternative (optional) electronic process of Identification/ KYC in paperless form, carried out by the reporting entities by undertaking seamless, secure, real-time with geo- tagging, consent based audio-visual interaction with the subscriber to obtain identification information including the necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the subscriber.

3.26 "Subscriber" shall have the meaning as per clause (t) of sub-section (1) of section 2 of the PFRDA Act. In these guidelines, the phrase Subscriber, Customer and Client has been used interchangeably and shall be considered to have the same meaning.

3.27 Words and expressions used and not defined in these guidelines but defined in the Pension Fund Regulatory and Development Authority Act, 2013, the PML Act, the PML Rules, the Aadhaar Act, Unlawful Activities (Prevention) Act, 1967 shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

4. Internal policies, procedures, controls, responsibility and compliance arrangement

4.1 Bank has to establish and implement policies, procedures, internal controls and formulate and implement a Client Due Diligence (CDD) Programme that effectively serve to prevent and impede Money Laundering (ML) and Terrorist Financing (TF).

4.2 To be in compliance with these obligations, the senior management of the Bank shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

The Bank shall:

4.2.1 Develop a KYC/AML/CFT program comprising of policies and procedures, for dealing with KYC, ML and TF reflecting the current statutory and regulatory requirements.

4.2.2 Ensure that the content of these guidelines are understood by all **employees, associated Retirement Advisers and Pension agents**, engaged in facilitating distribution of NPS / APY or any other pension scheme regulated or administrated by PFRDA and develop awareness and vigilance to guard against ML and TF amongst them.

4.2.3 The KYC/AML/CFT policy should have the approval of the Board of Directors or equivalent authority. The program and processes emanating from the Board approved policy shall be reviewed periodically on the basis of risk exposure and suitable changes (if any) be effected based on experience and to comply with the extant PML Act / PML Rules / Regulations / Guidelines and other applicable norms.

4.2.4 The Board of Directors or equivalent authority or Committee of the Board or the Senior Management Official(s) designated by the Board shall be apprised about the observations, violations, reporting etc., including follow-up action on periodic basis.

4.2.5 Undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of subscriber, business relationship or transaction.

4.2.6 Have in place a system for identifying, monitoring and reporting suspected ML or TF transactions to Financial Intelligence Unit – India(FIU-IND) and the law enforcement authorities in accordance with the guidelines issued by Government of India.

4.3 Policies and procedures set under KYC/AML/CFT program shall cover:

4.3.1 Communication of policies relating to prevention of ML and TF to all level of management and relevant staff that handle subscribers' information (whether in branches or departments) in all the offices of the Bank;

4.3.2 The Client Due Diligence Program including policies, controls and procedures, approved by the Board of Directors or equivalent authority or Committee of the Board or the Senior Management Official(s) designated by the Board to enable the Bank to manage and mitigate the risk that have been identified by the Bank;

4.3.3 Maintenance of records;

4.3.4 Compliance with relevant statutory and regulatory requirements;

4.3.5 Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;

4.3.6 Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of frontline staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of subscribers and other such factors.

4.4 Responsibility of the Bank:

The following steps are to be taken to strengthen the level of control on employees, business correspondents, associated Retirement Advisers, and **Pension agents** of the Bank:

4.4.1 Standard Operating Procedure/Guidance note/Process document covering

responsibilities of representatives of the Bank must be put in place. A clause to this effect should be suitably included as part of the contract(s) entered with them.

4.4.2 Bank shall initiate appropriate actions against defaulting representative who expose the Bank to KYC/AML/CFT related risks on multiple occasions.

4.4.3 If the Bank is engaging the services of individual like **Retirement advisors and Pension agents** for facilitating the distribution of pension schemes, the engagement process of such individuals shall be monitored scrupulously in view of set KYC/AML/CFT measures.

Regulation 44 (2) of PFRDA (PoP) Regulations, 2018 as amended, specifies that "A point of presence shall be liable for any acts of omission or commission, by the pension agents in discharge of its functions, arising out of such engagement, including compliance with KYC and AML norms prescribed under Prevention of Money Laundering Act, 2002, monitoring and supervising their activities, imparting training on pension schemes to them."

4.4.4 Financial groups shall be required to implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority- owned subsidiaries of the financial group:

- a) policies and procedures for sharing information required for the purposes of Customer Due Diligence and ML/TF risk management;
- b) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done). Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and
- c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

4.4.5 The overseas branches of the Bank to conduct client due diligence /AML standard for the subscribers specified by the PFRDA for the pension scheme regulated/administered by PFRDA. If the host country does not permit implementation of these guidelines, Bank should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform the same to PFRDA.

4.5 Certificate of Compliance:

Bank shall submit certificate of compliance as provided in Annexure 1 along with submission of Annual Compliance Certificate i.e., till 31st October of succeeding Financial Year.

5. Appointment of a Designated Director and a Principal Officer

5.1 A "Designated Director", who has to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules, shall be appointed or designated by the Bank.

5.2 A "Principal Officer" (PO) at a senior management shall be appointed to ensure compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules.

5.3 Any changes to the contact details (including mobile number, email ID and business address) of the Designated Director and the Principal Officer shall be communicated to PFRDA and FIU-IND within 30 days of its effect.

5.4 In terms of Section 13 of the PML Act, the Director, FIU-IND can take appropriate action, including imposing a monetary penalty on reporting entities or its Designated Director or any of its employees for failure to comply with any of its KYC/AML/CFT obligations.

6. Recruitment and Training

6.1 Adequate screening mechanism as an integral part of the Bank's personnel recruitment/hiring process shall be put in place.

6.2 On-going training programme shall be put in place so that the members/staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff, staff dealing with new subscribers. The frontline staff shall be specially trained to handle issues arising from lack of subscriber education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Bank, guideline and related issues shall be ensured.

7. Internal Control/Audit

Internal audit/inspection department of the Bank or the external auditor appointed by the Bank shall periodically verify compliance with the extant policies, procedures and controls related to money laundering activities on the basis of overall risk assessment. Bank shall also upgrade its questionnaire and system from time-to-time in accordance with the extant PML Act and PML Rules. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. Bank shall submit audit notes and compliance to the Audit Committee and in its absence directly to the Board or equivalent authority of the Bank.

8. Know Your Customer (KYC) Norms

8.1 KYC Norms

8.1.1 Bank should make best efforts to determine the true identity of subscriber(s).

8.1.2 Bank shall not allow the opening of or keep any anonymous account or account in fictitious names or whose identity has not been disclosed or cannot be verified. Effective procedures should be put in place to obtain requisite details for proper identification of new/existing subscriber(s).

8.1.3 Bank shall verify the identity, address and recent photograph in compliance with provision as specified in PML Rules.

8.1.4 At any point of time, where Bank is no longer satisfied about the true identity and the transaction made by the subscriber, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND), if it is satisfied that the transaction meets the criteria specified in sub clause (g) of clause (1) of Rule 2 of the PML Rules and guidelines / indicators issued by FIU-IND or PFRDA.

8.1.5 Bank may perform KYC process by any of the following methods:

8.1.5.1 Aadhaar based KYC through Online Authentication subject to notification by the

Government under section 11A of PML Act Or

8.1.5.2 Aadhaar based KYC through offline verification Or

8.1.5.3 Digital KYC as per PML Rules Or

8.1.5.4 Video Based Customer Identification Process (VCIP) as consent based alternate method of establishing the subscriber's identity using an equivalent e- document of any officially valid document (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 in Annexure I of PML Rules and the VCIP process for various activities under NPS as has been laid down by PFRDA vide circular no. PFRDA/2020/46/SUP-CRA/18 dated 6th October 2020 (Annexure 2) Or

8.1.5.5 By using "KYC identifier" allotted to the subscriber by the CKYCR Or

8.1.5.6 By "using Digilocker" as prescribed by the PFRDA vide circular no. PFRDA/2021/5/PDES/5 dated 3rd February 2021 (Annexure 3) Or

8.1.5.7 By using certified copy of an 'officially valid document' containing details of the identity and address, recent photograph and such other documents including financial status of the subscribers and

8.1.5.8 PAN/Form 60 (wherever applicable) and any other documents as may be required

8.1.6 It is imperative to identify and report cases where contribution is disproportionate to income.

8.2 Client Due Diligence (CDD)

Bank shall undertake CDD as per the provisions of Rule 9 of PML Rules. Accordingly, the Bank shall undertake CDD as follows:

8.2.1 Knowing new subscriber: In case of every new subscriber, necessary client due diligence with valid KYC documents of the subscriber shall be done at the time of commencement of account-based relationship/client-based relationship. Such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

8.2.2 Knowing existing subscribers

8.2.2.1 The AML/ CFT requirements are applicable for all the existing subscribers. Hence, necessary CDD with KYC (as per extant PML Rules) shall be done for the existing subscribers from time-to-time basis the adequacy of the data previously obtained. Further, periodic updation of KYC of NPS account shall be done as follows:

- a) In case of NPS Tier II accounts (excluding Tier II Tax Saver Scheme) - Every 3 years.
- b) In case of Tier II account, where subscriber is Politically Exposed Person (PEP) – Every 2 years.
- c) At the time of exit from NPS Tier I account.
- d) Whenever there is upward revision in the risk profile of the subscriber.
- e) As and when there are revision or changes in PML Act / PML Rules.

8.2.2.2 Where the risks of money laundering or terrorist financing are higher, Bank should conduct enhanced due diligence (EDD) measures, consistent with the risks identified.

8.2.2.3 Where Bank forms a suspicion of money laundering or terrorist financing, and it

reasonably believes that performing the Client Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file Suspicious Transaction Report (STR) with FIU-IND.

8.2.3 Ongoing Due Diligence: Besides verification of identity of the subscriber at the time of opening of pension account / initial contribution, risk assessment and ongoing due diligence should also be carried out at times when additional/ subsequent contributions are made. Any change which is inconsistent with the normal and expected activity of the subscriber should attract the attention of the Bank for further ongoing due diligence processes and action as considered necessary.

8.2.3.1 Bank shall identify the source of contribution and ensure that the contribution is being done through the subscriber's source of funds.

8.2.3.2 Verification at the time of exit (superannuation /premature exit / death etc.)

a) No payments should be made to third parties on attainment of superannuation except payments to nominee(s)/ legal heir(s) in case of death.

b) Necessary due diligence of the subscriber(s) / nominee(s) / legal heir(s) should be carried out before making the pay-outs/settling claims.

8.2.3.3 Notwithstanding the above, Bank is required to ensure that no vulnerable cases go undetected, especially, where there is suspicion of money- laundering or terrorist financing, or where there are factors to indicate a higher risk, necessary due diligence will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

9. Risk Assessment and Risk Categorization

9.1 While assessing the subscriber's risk profile under pensions schemes regulated/ administered by PFRDA, Bank may inter-alia take into account the following:

9.1.1 Whether contributions are mandatory contribution viz. Employees of central/state government/autonomous bodies/public sector undertakings covered under NPS (These accounts would generally involve lower risk)

9.1.2 Whether contributions are voluntary and low-contribution: APY being fixed and low contribution pension scheme and NPS Lite being low contribution pension scheme (These accounts generally involve lower risk)

9.1.3 Contributions towards NPS Tier I account on a voluntary basis (These accounts generally involve moderate risk)

9.1.4 Voluntary contributions towards NPS Tier II account, which is a withdrawable account (These accounts involve generally higher risk in comparison to other categories)

9.2 Notwithstanding anything contained in 9.1 above, while assessing the subscriber's risk profile, Bank shall consider the following factors:

9.2.1 Nature of account (For e.g. - NPS Tier I, NPS Tier II, NPS Tier II Tax Saver Scheme, NPS Lite, APY and any other scheme regulated/administered by PFRDA)

9.2.2 Source of contribution.

9.2.3 Mode of contribution (Cash / Online / Cheque / DD/ Card/ employers bank account etc.)

9.2.4 Regularity in the flow of contribution (For e.g. – Contributions under employer and

employee relationship)

9.2.5 Withdrawals under Tier I and Tier II account.

9.2.6 Residence status of subscriber (For e.g. – Subscribers residing in jurisdiction with higher national risk assessment)

9.2.7 Politically Exposed Person

9.2.8 Contributions made by the subscriber vis-à-vis the declared income/income range.

Above list is indicative and not exhaustive.

9.3 Bank have to carry out ML and TF Risk Assessment exercise as provided in sub rule (13) of Rule 9 of PML Rules based on risk exposure to identify, assess, document and take effective measures to mitigate its ML and TF risk for subscribers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. While assessing the ML/TF risk, the Bank is required to take cognizance of the overall sector specific and country specific vulnerabilities, if any, that the Government of India / PFRDA may share from time to time. Further, the internal risk assessment carried out by the Bank should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

9.4 The documented risk assessment shall be updated from time to time. The Bank shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. It shall be made available to competent authorities and law- enforcement agencies, as and when required.

9.5 Risk Categorization:

9.5.1 Risk categorization shall be undertaken based on parameters detailed at clause 9.1 and 9.2 besides others like subscriber's identity, nature of employment, high value deposits in Tier II account / in Tier I account near superannuation, unusual withdrawals in Tier II account etc. While considering subscriber's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. Bank shall ensure enhanced due diligence (EDD) for NPS Tier II account (except accounts under NPS Tier II Tax Saver Scheme).

9.5.2 For the purpose of risk categorization, individuals whose identities and source of income can be easily identified and transactions in whose pension accounts by and large conform to the known profile may be categorized as low-risk. For low-risk subscribers the PRAN account may require only the basic requirements like verifying the identity, current address, annual income and sources of fund of the subscriber are to be met. Notwithstanding the above, in case of continuing relationship, if the situation warrants, as for examples if the subscribers profile is inconsistent with the investment through subsequent contributions, a re-look on subscribers profile is to be carried out.

9.5.3 For the high-risk profiles, like for subscribers who are non - residents, high net worth individuals, Politically Exposed Persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC procedures should ensure higher verification and counter checks.

9.6 Risk assessment for New Business Practices/Developments:

9.6.1 Bank shall pay special attention to money laundering threats that may arise from

a) New business practices including new delivery mechanisms

b) Use of new or developing technologies for the pension schemes regulated/administered by the PFRDA.

9.6.2 Bank shall undertake the above risk assessment exercise, prior to the use of such practices and technologies and shall take appropriate measures to manage and mitigate the risks.

10. Simplified Due Diligence (SDD)

10.1 Simplified measures as provided under clause (d) of sub-rule (1) of Rule 2 of PML Rules are to be applied by the Bank in case of accounts opened under APY where the account is classified as Low Risk.

However, Simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high- risk scenarios apply, based on the Risk Assessment/categorization policy of the Bank.

10.2 The list of simplified due diligence documents are specified in clause (d) of sub- rule (1) of Rule 2 of the PML Rules.

11. Enhanced Due Diligence (EDD)

11.1 Enhanced Due Diligence as mentioned in Section 12AA of PML Act shall be conducted for high-risk categories of subscribers.

11.2 Bank should examine, as far as reasonably possible, unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, Bank should conduct enhanced due diligence measures, consistent with the risks identified.

11.3 Bank shall,

11.3.1 Verify the identity of the subscriber preferably using Aadhaar subject to the consent of subscriber or;

11.3.2 Verify the subscriber through other modes/ methods of KYC as specified through circulars / guidelines issued by the Authority from time to time.

11.4 Bank shall examine the ownership and financial position, including subscriber's source of funds commensurate with the assessed risk of subscriber and his/her profile.

12. Sharing KYC information with Central KYC Registry (CKYCR)

12.1 Government of India has notified the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

12.2 Bank is required to perform the CKYCR related functions **such as filing, retrieval, and utilisation of the KYC records with the Central KYC Records Registry or any other matter in connection with or incidental thereto**, in the manner as prescribed under the PML Rules. For the purpose of performing such functions Bank is required to get registered with CERSAI.

12.3 For the purpose of verification of identity of a client (Para 8.2) or on-going due diligence (Para 8.2.3), Bank shall seek the KYC Identifier from the client or retrieve the KYC Identifier, if available, from the Central KYC Records Registry and proceed to

obtain KYC records online by using such KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless

- a) there is a change in the information of the client as existing in the records of Central KYC Records Registry; or**
- b) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms prescribed by the Authority; or**
- c) the validity period of the downloaded documents has lapsed; or**
- d) Bank considers it necessary in order to verify the identity or address (including current address) of the client as per these guidelines, or to perform enhanced due diligence or to build an appropriate risk profile of the client.**

12.4 Bank after obtaining additional or updated information from the client during verification of identity of a client (Para 8.2) or On-going due diligence (Para 8.2.3), within seven (7) days or within such period as may be notified by the Central Government, furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client.

12.4.A If any update in the KYC record of an existing client is received by the Bank from Central KYC Records Registry as per Para 12.4, the Bank shall retrieve the updated KYC records from the Central KYC Records Registry and shall update the KYC record maintained by the Bank.

12.5 If the KYC identifier is not submitted by the subscriber or not available in the CKYCR portal, Bank shall capture the KYC information in the manner as prescribed under the PML Rules and as per the KYC Template stipulated for Individuals. The KYC template for ‘individuals’ and the ‘Central KYC Registry Operating Guidelines 2016’ for uploading KYC records on CKYCR finalised by CERSAI are available at www.ckycindia.in

12.6 Bank shall file the electronic copy of the subscriber’s KYC records with CKYCR within 10 days after the commencement of account-based relationship with a subscriber as per the guidelines / instructions / circulars by PFRDA from time to time.

12.7 Once “KYC Identifier” is generated/ allotted by CKYCR, the Bank shall ensure that the same is communicated immediately to the respective subscriber in a confidential manner, mentioning its advantage/ use to the subscriber.

12.8 The following details need to be uploaded on CKYCR if Verification / Authentication is being done using Aadhaar:

12.8.1 For online Authentication,

- a) The redacted Aadhar Number (Last four digits)

- b) Demographic details
- c) The fact that Authentication was done

12.8.2 For offline Verification,

- a) KYC data
- b) Redacted Aadhaar number (Last four digits)

12.9 At the time of periodic updation, it is to be ensured that all existing KYC records of subscriber are incrementally uploaded as per the extant CDD standards. Bank shall upload the updated KYC data pertaining to active pension accounts against which “KYC identifier” are yet to be allotted/generated by the CKYCR.

12.10 Bank shall not use the KYC records of the subscriber obtained from Central KYC Records registry for purposes other than verifying the identity or address of the subscriber and should not transfer KYC records or any information contained therein to any third party as per Rule 9(1F) of PML rules unless authorised to do so by the subscriber or PFRDA or by the Director (FIU- IND). Bank shall ensure that in case of accounts that have been opened prior to operationalisation of CKYCR, the KYC records are updated in the CKYCR during periodic updation and that the subscriber's accounts are migrated to current Customer Due Diligence Standards (CDD).

12.11 Bank shall submit the MIS related to the CKYC data upload/download etc. to PFRDA as stipulated from time to time.

13. Reliance on third party KYC

13.1 For the purposes of KYC norms under clause 8, while Bank is ultimately responsible for subscriber due diligence and undertaking enhanced due diligence measures, as applicable, Bank may rely on a KYC done by a third party subject to the conditions specified under sub-rule (2) of rule (9) of the PML Rules.

13.2 Bank can utilise the SEBI KRA for KYC in accordance with PFRDA circular PFRDA/2019/16/PDES/2 dated 23rd September 2019 (Annexure 4)

13.3 The ultimate responsibility for relying on third party KYC is with the Bank.

14. Pension accounts of Politically Exposed Persons (PEPs)

14.1 The proposals of Politically Exposed Persons (PEPs) in particular requires examination by senior management of the Bank.

14.2 Bank should lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are family members, close relatives/associates of PEPs. These measures are also to be applied to pension accounts of which a PEP is the beneficiary/nominee.

14.3 If the on-going risk management procedures indicate that the subscriber or beneficiary is found to be PEP or subsequently becomes PEP, the senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

14.4 Bank to take reasonable measures to determine whether the beneficiaries of a pension account are PEPs at the time of the exit, and should ensure the internal controls are in place. While processing exit request, Bank should apply risk-based monitoring of such withdrawal to determine if the recipient of the funds is a PEP.

14.5 Bank shall undertake reasonable measures to establish the source of wealth and the source of funds of customers identified as PEPs.

15. Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)

15.1 Section 51A of the Unlawful Activities (Prevention) Act, 1967(UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated 2nd February 2021 detailing the procedure for the implementation of Section 51A of the UAPA.

15.2 The Bank should not open pension account of a subscriber whose identity matches with any person in the UN sanction list and those reported to have links with terrorists or terrorist organizations.

15.3 Bank shall periodically check MHA website for updated list of banned individuals.

15.4 Bank shall maintain an updated list of designated individuals in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals are holding any pension accounts. An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list and UNSC 1988 can be accessed regularly from the United Nations website at <https://www.un.org/securitycouncil/sanctions/1988/materials>.

15.5 By virtue of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. [The list is accessible at website <http://www.mha.gov.in>]. To implement the said section an order reference F. No. 14014/01/2019/CFT dated 2nd February, 2021 has been issued by the Government of India. The salient aspects of the said order with reference to insurance sector would also be applicable to NPS / NPS Lite / APY or any other scheme regulated or administered by PFRDA.

15.6 The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

16. Prospects residing in the jurisdiction of countries identified as deficient in AML/CFT regime

16.1 Bank shall specifically apply enhance due diligence(EDD) measures, proportionate to the risks, to business relationships and transactions with individual from countries for which this is called for by the FATF.¹⁰

16.2 Pay special attention to unusual contributions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings have to be maintained for assisting competent authorities.

16.3 Agents / intermediaries / employees to be appropriately informed to ensure compliance with this stipulation.

16.4 Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations.

16.5 Take similar measures on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

17. Reporting Obligations

17.1 NPS being an unbundled architecture where Central Recordkeeping Agency (CRA) maintains the records centrally for all the transactions, CRA is responsible for filing of reports to Director, FIU-IND in accordance with PML Rules.

17.2 In addition to the above every reporting entity should register with Financial Intelligence Unit - India (FIUIND) under the regulator "PFRDA", and shall also furnish to the Director, Financial Intelligence Unit- India (FIU-IND), information referred to in Rule 3 (Maintenance of records of transactions (nature and value)) in terms of Rule 7 (Procedure and manner of furnishing information) of the PML (Maintenance of Records) Rules, 2005.

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

17.3 The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist 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.

17.4 Red Flag Indicators issued by FIU-IND also be taken in account for Suspicious Transaction, wherever necessary.

17.5 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 subscriber at any level. Confidentiality requirement does not inhibit information sharing among entities in the group.

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

17.7 Bank shall leverage the broadest number of data points / records available with them in implementing alert generation systems to assist in identifying and reporting suspicious activities.

17.8 Bank should not enter into arrangement with any unregulated entity which may have the effect of directly or indirectly impairing any reporting obligations of the Bank.

18. Record Keeping

18.1 In view of Rule 5 of the PML rules, Bank's Designated Director, Principal Officer, employees are required to maintain the information/records of types of all transactions [as mentioned under Rules 3 and 4 of PML Rules 2005] as well as those relating to the verification of identity of subscribers for a period of five years. The records referred to in the said Rule 3 shall be maintained for a period of five years from the date of transaction. Records pertaining to all other transactions, (for which Bank is obliged to maintain records under other applicable Legislations/Regulations/Rules) Bank shall retain records as provided in the said Legislation/Regulations/Rules but not less than for a period of five years from the date of end of the business relationship with the subscriber.

18.2 Records can be maintained in electronic form and/or physical form. In cases where services offered by a third-party service providers are utilized,

18.2.1 Bank shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

18.2.2 The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored and recorded.

18.2.3 The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

18.2.4 It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.

18.3 Bank should implement specific procedures for retaining internal records of transactions, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Bank should retain the records of those accounts, which have been settled by claim, for a period of at least five years after that settlement.

18.4 In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, Bank is required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.

18.5 In case of subscriber identification, data obtained through the subscriber due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

19. Monitoring of Transactions

19.1 Regular monitoring of transactions is vital for ensuring effectiveness of the

KYC/AML/CFT procedures. This is possible only if the Bank have an understanding of the normal activity of the subscriber so that it can identify deviations in transactions/activities.

19.2 Bank shall pay special attention to all complex large transactions/ patterns which appear to have no economic purpose. The Bank may specify internal threshold limits for each class of subscriber accounts and pay special attention to transactions which exceeds these limits. The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to PFRDA/ FIU-IND/ other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction.

19.3 The Principal Officer of the Bank shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU- IND.

19.4 Further, Compliance Department shall randomly examine a sample of transactions undertaken by subscribers to comment on their nature i.e., whether they are in nature of suspicious transactions or not.

Annexure 1
(As specified in Para 4.5)

Certificate of Compliance with respect to KYC/AML/CFT

Name of Reporting Entity:

Financial Year:

We do hereby submit that..... (name of the Bank)
has fully complied with all the norms laid down by PFRDA and with the extant PML
Act/PML Rules.

Designated Director (Name and Signature along with the stamp of the entity)

(* to be submitted along with submission of Annual Compliance Certificate)



**पेंशन निधि विनियामक और
विकास प्राधिकरण**

बी-14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली-110016
दूरभाष : 011-26517501, 26517503, 26133730
फैक्स : 011-26517507
वेबसाइट : www.pfrda.org.in

**PENSION FUND REGULATORY
AND DEVELOPMENT AUTHORITY**

B-14/A, Chhatrapati Shivaji Bhawan,
Qutub Institutional Area,
Katwaria Sarai, New Delhi-110016
Ph : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

CIRCULAR

CIR No.: PFRDA/2020/46/SUP-CRA/18

Date: October 06, 2020

To,

All stakeholders under NPS

Subject: Video based Customer Identification Process (VCIP) for NPS

PFRDA in its endeavor to make the subscriber on-boarding , exit, processing of service requests and contribution deposits seamless and subscriber friendly, has been constantly introducing new modes of subscriber KYC and authentication processes such as OTP/ eSign, Offline Aadhaar based KYC, third party reliance for KYC, Paperless on-boarding, e- exit for eNPS Subscribers, e Nomination, D Remit etc.

2. In continuation of such efforts, it has now been decided to permit intermediaries registered with PFRDA to use Video based Customer Identification Process (VCIP) for the purpose of on-boarding, exit or any other service request related to NPS.

3. The envisaged benefits of VCIP are as under -

- i. In the new normal world post COVID, VCIP overcomes the challenges of remote presence, limited mobility, contactless services, social distancing norms etc.
- ii. It eases the process of on-boarding/ exit / other service requests, as the Subscriber verification is carried out without the need of physical presence of Subscribers before Point of Presence (PoPs)/Nodal officers.
- ii. It optimizes the turnaround time of account opening, execution of exit and processing of other service requests.

- iii. It provides the opportunity for expanding the reach of NPS since account opening process is paperless, instantaneous, convenient and cost effective.
 - iv. Several PoPs which have recently been registered with PFRDA are functioning online and do not have any physical presence across locations. VCIP shall enable these PoPs to source Subscribers under NPS with greater ease, service them and carry out exit process with proper due diligence.
 - v. Since OTP/eSign based authentication is a part of VCIP, the process is paperless.
4. While the PoPs registered with other Financial Sector Regulators may comply with VCIP guidelines issued by those regulators, the POPs which are registered solely with PFRDA and wish to adopt VCIP, shall adhere to the process given in the **Annexure**.
5. The PoPs, in association with Central Record Keeping Agencies(CRAs) are advised to build an online platform for developing VCIP in the interest of subscribers at the earliest.
6. The duties and responsibilities of POPs are detailed in Regulation 15 of PFRDA (Point of Presence) Regulations 2018.



(K. Mohan Gandhi)
General Manager

Annexure

Basic features of VCIP under NPS

A. Mobile Application based VCIP

1. POPs implement their own mobile application for undertaking VCIP.
2. This application shall facilitate taking photograph, scanning of documents, upload of OVD (Officially Valid Document) through Digilocker/other OVDs as specified by PFRDA, capturing the signature during VCIP in live environment.
3. The usage of the application is only by authorized person of the PoP and not by any 3rd party.
4. The application shall also have features of random action initiation for Subscriber's response to establish that the interactions are not prerecorded. Further, the application should have time stamping and geo-location tagging to ensure physical location in India etc.
5. PoPs shall ensure that the process is seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the subscriber and the quality of the communication is adequate to allow for establishing the identity of customer beyond doubt.
6. PoPs shall carry out the liveness check in order to guard against spoofing and other fraudulent manipulations. POPs shall carry out software and security audit and validation of their App performing VCIP.
7. PoPs can add additional safety and security features, other than prescribed above.
8. PoPs should ensure Instant bank account verification through penny drop, to verify the beneficiary bank details is mandatory.
9. The photo/signature of the subscriber is to be uploaded during VCIP while On-boarding. During exit, the withdrawal document along with KYC needs to be uploaded for the purpose of issuing annuity by Annuity Service Providers. The soft copies of CSRF needs to be generated and shared with CRA and the subscribers. For rest of services, the subscribers can upload required documents for verification by PoPs through VCIP.

B. Non Mobile Application Based VCIP:

1. PoPs through their authorized official, specifically trained for this purpose, may undertake live VCIP of an individual subscriber/applicant, after obtaining their informed consent. The activity log along with the credentials of the person performing the VCIP shall be stored securely along with time stamping for easy retrieval and scrutiny.
2. The VCIP shall be only in a live environment.



3. The VCIP shall be clear and undisturbed. Further, the NPS Subscriber/applicant in the video shall be easily re-cognizable and shall not be covering their face in any manner.
4. The VCIP process shall include random question and response from the NPS Subscriber/applicant including displaying the OVD as specified by PFRDA in its CSRF/Exit Form/Service request forms.
5. PoPs shall ensure that photograph of the Subscriber provided in KYC documents/PRAN card/CSRF, as the case may be, matches with the Subscriber during VCIP.
6. Video call must be from the domain of the concerned PoP and not from a third-party sources.
7. PoPs should ensure Instant bank account verification through penny drop, to verify the beneficiary bank details is mandatory.
8. PoPs can add additional safety and security features, other than prescribed above.
9. The photo/signature of the subscriber is to be uploaded during VCIP while On-boarding. During exit, the withdrawal document along with KYC needs to be uploaded for the purpose of issuing annuity by Annuity Service Providers. The soft copies of CSRF needs to be generated and shared with CRA and the subscribers. For rest of services, the subscribers can upload required documents for verification by PoPs through VCIP.



Circular


Circular No: PFRDA/2021/5/PDES/5

Date: 3rd February 2021

To
Central Recordkeeping Agencies
Points of Presence &
National Pension System Trust

Subject: DigiLocker for National Pension System services

1. Government of India has introduced DigiLocker facility where citizens can get authentic documents/ certificates in digital format from original issuers of these certificates. This key initiative enhances effectiveness of service delivery, making these hassle-free and friendly for the citizens.
2. As per Rule 9(4)(ab) of PML Rules, 2005 for the purpose of client due-diligence (i.e. KYC verification) process, an individual can submit '*any officially valid document or the equivalent e-document thereof containing the details of his identity and address*' to the reporting entity (Points of Presence in case of NPS), along with PAN.
3. In light of the above, CRAs and PoPs are advised to provide DigiLocker as an option for applicants/subscribers to submit documents (Officially Valid Documents available in Digilocker) required for NPS onboarding/sector shifting or exit through digital methods. As the documents/ certificates in Digilocker are from the original issuers, the certificates / documents directly obtained from DigiLocker would not also require further verification.
4. The details/process for integration with DigiLocker is Annexed.


(Mono MG Phukon)
General Manager

Annex

Implementation of DigiLocker in Government Departments for Citizen Centric Services

The entities need to register themselves as mentioned below and refer to the technical documents for integration of NPS services with DigiLocker.

1. **Registration:** Authorized officials have to visit the 'Partner portal' of DigiLocker ([url:https://partners.digilocker.gov.in](https://partners.digilocker.gov.in)) and register as an Issuer, requester or verifier.
2. **Technical resource for integration:** API specification documents are available at below link: <https://digilocker.gov.in/resource-center.html>
3. For any Technical support/ guidance please write to: partners@digitallocker.gov.in
4. Contact details of officials for escalation:

Level-1

Sh. Durgaprasad Dash,
Addl. General Manager,
email: durga@digitalindia.gov.in

Level-2

S Debabrata Nayak,
Project Director, NeGD
email: dnayak@digitalindia.gov.in



PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

CIRCULAR

CIR No.: PFRDA/2019/16/PDES/2

Date: 23rd September 2019

To
All Stakeholders under NPS

Subject: Utilization of SEBI KRAs by PoPs for onboarding of subscriber in National Pension System (NPS).

1. The Points of Presence (PoPs) registered under PFRDA (PoP) Regulations, 2018 acts as the interface between the subscriber and the NPS architecture while the PoP performs its functions related to registration, Know Your Customer (KYC) verification, receiving contributions and servicing subscribers' requests.
2. Few PoPs which are also registered with SEBI and having access to KRA have requested PFRDA to permit them to utilize SEBI KRA for onboarding subscribers in NPS as this would eliminate duplication of KYC processes and will facilitate ease of onboarding subscribers in NPS.
3. The Authority after due examination of the requests has now approved that the PoPs having access to SEBI KYC Registration Agencies (KRAs) may utilize the same as an additional method of KYC authentication while onboarding subscribers in NPS. When a PoP adopts this method for completing KYC, the PoP (reporting entity) would be considered to be relying on third party for 'client due diligence' as provided under Sub rule 2 of Rule 9 of PML (Maintenance of Records) Rules, 2005 (as amended for time to time) and shall be bound by the conditions mentioned thereunder. SEBI has provided its no objection to allow PFRDA registered Points of Presence to access the KYC information from the KRA system vide its letter no SEBI/HO/MIRSD/DOP/OW/P/21350/2019 dated 20th August 2019.
4. It may be noted that PoP will be ultimately responsible for the 'client due diligence' and undertaking enhanced due diligence measures, as applicable under the PML Rules and the PFRDA (PoP) Regulations 2018 while onboarding subscriber in NPS.


(Mono MC Phukon)
General Manager