AML & CFT Guidelines
For
Trust and Company Service Providers (TCSPs)

Table of Contents

Acronyms 3

1. Background 4

2. Scope 6

3. Effective Date 6

4. General Obligations of Relevant Persons 6

4.1. Policies and Procedures to Combatting Money Laundering, Countering Terrorist Financing and Combatting Proliferation Financing (AML/CFT/CPF Program)……6

4.2. Internal policies, procedures, and controls to be implemented by relevant persons……..7

4.3. Registration of Reporting Entities, Appointment of Designated Director and Principal Officer……7

4.4. Internal Control/Audit……8

4.5. Know Your Customer (KYC) Norms 8

4.6. Periodic Updation of KYC…….. 11

4.7. Client due Diligence (CDD) Norms 11

4.8. Enhanced Due Diligence (EDD) Norms 14

4.9. Sanctions screening for notified activities 17

4.10. Obligation under the Unlawful Activities (Prevention) Act, 1967 17

4.11. Obligation under weapons of Mass Destruction Act, 2005 18

5. Transaction Monitoring and Reporting of STR to FIU-IND……. 20

6. Confidentialty…… .. 21

7. Prohibition on Tipping-off 21

8. Maintenance of Records 22

9. Risk Assessment 22

10. Access to Information under Section 12 of PMLA 24

11. Tracking Regular updates through Finnet and Website…… 25

Acronyms

Term	Definition
AML	Anti-Money Laundering
CFT	Countering the Financing of Terrorism
CDD	Customer Due Diligence
CPF	Combating Proliferation Financing
CKYCR	Central Know Your Customer Registry
CRS	Common Reporting Standards
DNFBP	Designated Non-Financial Business and Profession
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU-IND	Financial Intelligence Unit – India
KYC	Know Your Customer
ML/TF/PF	Money Laundering, Terrorism Financing and Proliferation Financing
NRA	National Risk Assessment
OVD	Officially Valid Document
PEPs	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act 2002
PMLR	Prevention of Money-laundering (Maintenance of Records) Rules 2005
RBA	Risk-Based Approach
RE	Reporting Entities
STR	Suspicious Transaction Report
UAPA	Unlawful Activities (Prevention) Act, 1967
UNSC	United Nations Security Council

Introduction

1. Background

1.1 The present document shall be referred to as the AML & CFT Guidelines (hereinafter called "The Guidelines") in respect of activities carried out by reporting entities (RE), as notified by the Central Government, vide notification S.O. 2135(E) dated May 09, 2023, (hereinafter called "The Notification"). For the purpose of the present guidelines, money laundering has the same meaning as in Section 3 of Prevention of Money-Laundering Act, 2002 ('PMLA').

1.2 PMLA lays down record-keeping and reporting obligations for financial institutions and persons carrying on designated business or profession, with the latter defined in sub-clause (vi) of clause (sa) of sub-section (1) of section 2 which states that 'person carrying on designated business or profession', includes persons carrying on such other activities as the Central Government may, by notification, designate from time- to-time. In exercise of said powers, the Central Government, vide "The Notification", notified certain activities when carried out in the course of business on behalf of or for another person, as the case may be, that are generally undertaken by "Trust and Company Service Providers (TCSPs)" thereby classifying them as Reporting Entities ("RE") under these guidelines.

1.3 The present document aims to provide a summary of legal provisions of anti-money laundering, counter-terrorism financing and proliferation financing legislations in India, viz. the Prevention of Money Laundering Act, 2002 (hereinafter referred to as the "PMLA"), the Unlawful Activities (Prevention) Act, 1967 (hereinafter referred to as the "UAPA"), the Weapons of Mass Destruction and Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (hereinafter referred to as the "WMDA") and rules/notifications thereunder and to lay down steps that a relevant person carrying out certain financial transactions, on behalf of their clients, as notified vide Central Government, vide notification S.O. 2135(E) dated May 09, 2023, (*hereinafter referred to as 'Relevant Persons')*, shall implement to prevent, detect and report money laundering, terrorist financing or proliferation financing activities.

1.4 The Prevention of Money Laundering Act, 2002 (PMLA) brought into force with effect from 1st July, 2005, is applicable to all the Reporting Entities (RE) as defined in the said Act. Section 11A of the PMLA requires the reporting entities to verify the identity of their clients and the beneficial owners. Section 12 of the PMLA places certain obligations on the reporting entities which are as follows

a) Maintain a record of all transactions, including information relating to transactions covered under clause(b), in such manner as to enable it to reconstruct individual transactions;

b) Furnish to Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value as may be prescribed.

c) Maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

1.5 The Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR) have been framed under the PMLA. Rule 3 of the PML Rules prescribes the transactions, the records of which are to be maintained. Rule 7 of the PML Rules prescribes the procedure and manner of furnishing information, including obligation on reporting entities to evolve an internal mechanism for detecting the transactions prescribed in Rule 3. Rule 8 of the PML Rules prescribes the time of furnishing such information and Rule 9 of the said Rules prescribes Client Due Diligence procedure and manner of verification of records of identity of clients, to take reasonable steps to understand the nature of customer's business, its ownership and control, and identification and verification of the beneficial owners. The RE, its Designated Director, officers and employees are responsible for omissions and commissions in relation to the reporting obligations under Chapter IV of the PMLA.

1.6 **Relevant Persons**

The Central Government vide "The Notification", has notified the following activities, when carried out in the course of business on behalf of or for another person, as the case may be, as an activity for the purposes of sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the Prevention of Money-laundering Act, 2002 (15 of 2003):

(i) acting as a formation agent of companies and limited liability partnerships;

(ii) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a firm or a similar position in relation to other companies and limited liability partnerships;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company or a limited liability partnership or a trust;

(iv) acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another type of trust; and

(v) acting as (or arranging for another person to act as) a nominee shareholder for another person.

Explanation:- For removal of doubts, it is clarified that the following activities shall not be regarded as activity for the purposes of sub-clause (vi) of clause (sa) of sub-section (1) of section 2 of the Act, namely–

(i) any activity that is carried out as part of any agreement of lease, sub-lease, tenancy or any other agreement or arrangement for the use of land or building or any space and the consideration is subjected to deduction of income-tax as defined under section 194-I of Income-tax Act, 1961 (43 of 1961); or

(ii) any activity that is carried out by an employee on behalf of his employer in the course of or in relation to his employment; or

(iii) any activity that is carried out by an advocate, a chartered accountant, cost accountant or company secretary in practice, who is engaged in the formation of a company to the extent of filing a declaration as required under clause (b) of sub- section (1) of section 7 of Companies Act, 2013 (18 of 2013);

(iv) or any activity of a person which falls within the meaning of an intermediary as defined in clause (n) of sub-section (1) of section 2 of the Prevention of Money- laundering Act, 2002 (15 of 2003).

2. Scope

The guidelines apply to financial transactions carried out by relevant persons as notified vide '***The Notification'***.

3. Effective Date

These guidelines shall take effect immediately i.e. from April 21, 2026.

4. General Obligations of Relevant Persons.

4.1. Policies and Procedures to Combatting Money Laundering, Countering Terrorist Financing and Combatting Proliferation Financing: (AML/CFT/CPF Program)

In order to discharge the statutory responsibility to detect possible attempts of money laundering, financing of terrorism or proliferation financing, every RE must have a robust AML/CFT/CPF program in place, which shall include the points mentioned in these guidelines. Rule 7(3) of the PMLR casts an obligation on every reporting entity

(RE) to evolve an internal mechanism to detect transactions as specified under Rule 3(1) and furnishing information about such transactions to FIU-IND.

4.2. Internal policies, procedures, and controls to be implemented by relevant persons

To comply with the obligations of Reporting Entities as specified under PMLA, PMLR, REs carrying out activities as notified under "The Notification" shall establish appropriate policies and procedures for the prevention of ML, TF, and PF, and ensure their effectiveness and compliance with all relevant legal and regulatory requirements. The reporting entities shall:

4.2.1 Issue a statement of policies and procedures for dealing with ML, TF and PF risks, reflecting the current statutory and regulatory requirements and

4.2.2 Periodically review the policies and procedures on the prevention of ML, TF, and PF to ensure their effectiveness.

4.2.3 Adopt client acceptance policies and procedures and undertake Client Due Diligence (CDD) measures in respect of the activities notified vide "The Notification";

4.2.4 Further, in terms of Rule (3A) of PMLR with regard to implementation of policies by groups (as per rule 2(1)(cba) of PMLR "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), Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PMLA.

4.3. Registration of Reporting Entities, Appointment of Designated Director and Principal Officer

4.3.1 A "Designated Director" (as defined under the PMLR as amended from time to time) shall be appointed to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

4.3.2 A Principal Officer (PO) at management level and preferably not below the level of Head (Audit/Compliance)/Chief Risk Officer or equivalent shall be appointed to ensure implementation and compliance with the obligations imposed under chapter IV of the Act and the Rules.

4.3.3 The Principal Officer and the Designated Director should be separate individuals. The contact details of the Designated Director and the Principal

Officer for AML/CFT/CPF obligations shall be communicated to FIU-IND at the earliest.

4.3.4 Roles and Responsibilities of Designated Director and the Principal Officer

The Designated Director and the Principal Officer shall be responsible for the following obligations to combat money laundering/ countering the financing of terrorism/ combat proliferation financing

4.3.4.1 The information in respect of a suspicious transaction shall be furnished promptly on the Principal Officer being satisfied that the transaction is suspicious as per Rule 8(2) of the PMLR. Such information shall include any attempted transactions, whether or not made in cash

4.3.4.2 Evolving an internal mechanism with regard to any directions/ guidelines as prescribed under sub rule (1) of Rule 3 of the PMLR

4.3.4.3 Communication of entity/group wide policies relating to prevention of ML, TF and PF to all management and relevant staff that handle account information, money and client records, etc. within their organisation

4.3.4.4 Implementation of other internal policies as drawn up under para 4.3 of these guidelines and, including Maintenance of records; Compliance with relevant statutory and regulatory requirements; Cooperation with the relevant law enforcement authorities, including the timely disclosure of information; Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML, TF and PF, including detection of suspected money laundering transactions.

4.4. Internal Control/Audit

There should be internal audit to ascertain on a regular basis, compliance with policies, procedures and controls relating to AML/CFT/CPF

4.5. Know Your Customer (KYC) Norms

4.5.1 All REs carrying out transactions as notified under “The Notification” must have a robust mechanism in place for complying with KYC requirements prior to on boarding of clients as well as for carrying out re-KYC and continued due diligence (CDD) of existing customers. Effective procedures should be put in place to obtain requisite details for proper identification of new customers as

well as existing customers (if such details are not already in place). Special care has to be exercised to ensure that the services are not availed under anonymous, pseudonymous, or fictitious names. REs carrying out activities as notified under "The Notification" are to take steps to identify the ultimate beneficial owner and take all reasonable measures to verify the identity to their satisfaction, in accordance with the provisions of the PMLA and the PMLR. For the purpose of these guidelines, Beneficial Ownership has the same meaning as in Rule 9(3) of PMLR. As such, 'beneficial owner' for this purpose means 'the natural person who has a controlling ownership interest or who exercises control through other means or the natural person on whose behalf a transaction is being conducted and includes a natural person who exercises ultimate effective control over a legal person'.

4.5.2 For the purpose of KYC, the Permanent Account Number (PAN) as applicable to residents or any other equivalent document for non-residents and any of the Officially Valid Document (OVD) as prescribed below can be used as a measure of identification

- The passport,
- The driving license,
- Proof of possession of Aadhaar number,
- The Voter's Identity Card issued by the Election Commission of India,
- Job card issued by NREGA duly signed by an officer of the State Government and
- Letter issued by the National Population Register containing details of name and address.

4.5.3 Further, documents or the equivalent e-documents thereof, in respect of the nature of business and financial status of the client shall also be obtained. Provided that,

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

ii. Where the OVD furnished by the customer does not have the updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

- Property or Municipal tax receipt;
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
- Letter of allotment of accommodation from employer 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;

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

iv. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

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

v. REs carrying out activities as defined under "The Notification" are required to comply with the relevant record keeping and reporting requirements under Information Technology Act and Income Tax Act in addition to record keeping and reporting requirements under PMLA and PMLR.

4.5.4 The officially valid documents (OVDs) must be verified by REs as defined under "The Notification".

4.5.5 In cases where e-KYC services of the Unique Identification Authority of India (UIDAI) are availed for KYC verification (which is acceptable subject to specific and express consent of the customer to access his/her data through UIDAI system), certification requirements under this clause shall be deemed to be complied with. The e-KYC should be based on biometric (finger/iris) authentication as the primary mode with One Time Password (OTP) based authentication as a second factor.

4.5.6 While implementing the KYC norms on legal persons, REs carrying out activities

as defined under "The Notification" will have to identify and verify their legal status through various documents, to be collected in support of

i. The name, legal form, proof of existence,
ii. Powers that regulate and bind the juridical persons,
iii. Address of the registered office/ main place of business
iv. For the purpose of KYC for business entities, documents mentioned in the Customer Due Diligence (CDD) measures prescribed in "The Guidelines", shall be used and maintained.

4.5.7 At any point in time during the period, where the REs carrying out transactions as defined under "The Notification" is no longer satisfied about the true identity of the customer, a Suspicious Transaction Report (STR) should be filed with FIU-IND

4.6 Periodic Updation of KYC

REs shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of REs' internal KYC policy. KYC shall be done by REs prior to taking on a customer engagement as well as a one-time exercise in cases where such KYC is not already present as on the date of issuance of these guidelines. REs carrying out activities as notified under "The Notification", may rely on the identification and verification steps that they have already undertaken in case of a customer, unless they have doubts about the veracity of the information with them. In cases where the appropriate CDD measures to identify the profile of a client cannot be applied or it is not possible to ascertain the identity of the client, or the information provided by the client is suspected to be false or non–genuine, RE, shall not enter into an engagement/ transaction with such a client. In such cases, a suspicious activity report shall be filed with FIU-IND

4.7 Client due Diligence (CDD) Norms

4.7.1 Relevant persons as notified under 'the notification', should maintain accurate and up-to-date customer information. REs carrying out activities as notified under "The Notification" should maintain accurate and up-to-date customer

information. In consonance with the basic principles of the KYC norms as prescribed in the PMLA or the rules made there under, all REs carrying out activities as notified under "The Notification" shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices. In accordance with Rule 9 of the PMLR, each RE carrying out activities as notified "The Notification" shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA, related to the 'Client Due Diligence Process'.

4.7.2 REs carrying out activities as notified under "The Notification" would be expected to make use of relevant measures to:

i. Perform robust client due diligence process on clients/beneficial owners/authorized signatories/counterparties;
ii. Since the clients of services offered could include international parties, adequate background checks including but not limited to financial and criminal checks may be carried out prior to accepting such client engagements.
iii. Identify risk-related details about the client through sanctions screening providers;
iv. Store customer KYC information for up to five years;
v. Submit reports to FIU-IND on a timely basis or upon request.
vi. All identification documents secured through the CDD measures should be retained by for a period of at least five years as required under the PMLA.
vii. The extent of the ongoing CDD measures applied should be determined on a risk-sensitive basis.
viii. However, it should be kept in mind that as a business relationship develops, the associated ML/TF/PF risks may change.

4.7.3 RE shall ensure that for a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

i. Certificate of incorporation
ii. Memorandum and Articles of Association
iii. Permanent Account Number of the company
iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

v. Documents, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

vi. the names of the relevant persons holding senior management position; and the registered office and the principal place of its business, if it is different.

4.7.4 RE shall ensure that for a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:

i. Certificate of incorporation

ii. Memorandum and Articles of Association

iii. Permanent Account Number of the company

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

v. Documents, relating to beneficial owner, the managers, officers or employees,as the case may be, holding an attorney to transact on the company's behalf

4.7.5 RE shall ensure that for a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained.

i. Registration certificate

ii. Trust deed

iii. Permanent Account Number or Form No.60 of the trust

iv. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

v. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust

vi. address of the registered office of the trust; and

vii. list of trustees and documents, as specified in paragraph 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

viii. REs shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. REs shall also maintain such registration records for a period of five years after the business relationship between

the customer and the RE has ended or the account has been closed, whichever is later.

4.8. Enhanced Due Diligence (EDD) Norms

4.8.1 REs carrying out activities as notified under "The Notification" should examine, as far as reasonably possible, the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering, terrorist financing or proliferation financing are higher, they must conduct enhanced due diligence, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

4.8.2 Conducting enhanced due diligence should not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than normal KYC. These measures should be commensurate with the risk. While not intended to be exhaustive, the following are some of the reasonable measures in carrying out enhanced due diligence:

i. More frequent review of the customers' profile/ transactions More frequent review of the customers' profile/ transactions
ii. Application of additional measures like gathering information from publicly available sources or otherwise.
iii. Reasonable measures to know the customer's source of funds commensurate with the assessed risk of customer and product profile which may include:
iv. Conducting independent enquiries on the details collected on/provided by the customer where required,
v. Consulting a credible database, public or other, etc.

4.8.3 Due to the potential for increased anonymity or obfuscation of financial flows and the challenges associated with conducting effective supervision and CDD, including customer identification and verification, the activities listed below are regarded as posing high ML/TF/PF risks that may potentially require the application of monitoring and EDD measures, where appropriate.

i. Application of EDD measures to business relationships and transactions with natural and legal persons from higher risk jurisdictions specifically with countries designated as tax-havens and those on the FATF grey and black lists.

ii. Implementation of EDD procedures when entering into business relationships with Politically Exposed Persons ("PEPs"). For the purposes of these guidelines 'PEP' shall have the same meaning assigned to it as per rule 2(1) (db) of PMLR.

iii. It must be ensured while carrying out EDD that the staff handling these sensitive formations should be well trained to prevent internal "tipping-off".

4.8.4 **Identification of Beneficial Owner:** RE shall ensure that 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 :-

(i) 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-

a) Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

b) "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. RE may decide to lower the threshold from 10% for identification of beneficial ownership where the company is incorporated in "High-Risk" jurisdictions or any other reason defined in its internal risk assessment.

c) In the specific scenario where no natural person holds the required percentage of shares or capital, the BO is identified as follows:

Step 1: <u>Control through Other Means</u>

If no one meets the ownership threshold, the institution must identify any natural person(s) exercising control of the legal person through other means.

This includes individuals with the power to appoint the majority of senior management, those with significant influence over strategic decisions, or those controlling the entity through debt instruments or informal means (e.g., personal connections).

Step 2: Senior Managing Official (SMO)

If no natural person can be identified under the first two criteria (ownership or other means of control), the Senior Managing Official (SMO) must be identified and recorded as the beneficial owner. The SMO is typically the individual responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal person, such as a CEO or Managing Director

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

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

(iii) Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustees, 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.

4.8.5 **Politically Exposed Persons:** REs shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

i. REs have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

ii. Reasonable measures are taken by the REs for establishing the source of funds / wealth;

iii. All such PEPs are subjected to enhanced monitoring on an on-going basis;

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

Explanation: For the purpose of this paragraph, "Politically Exposed Persons"

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

4.9. Sanctions screening for notified activities

4.9.1 For the purpose of enhanced monitoring, sanctions screening should be carried out both at the time of on boarding as well as when any of the notified activities are carried out.

4.9.2 REs carrying out transactions as notified under "The Notification", must ensure prompt application of the directives when issued by the competent authorities for implementing United Nations Security Council Resolutions, as well as national sanctions, relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions.

4.9.3 Prompt application of the directives when issued by the competent authorities relating to the individuals designated as 'terrorist' under Section 35(1)(a) of the UAPA, 1967 and directives when issued by the competent authorities under WMDA, must be ensured. In this regard, following safeguards may be put in place :-

i. Ensuring that client engagements related to the notified activities, are completed only after appropriate sanctions screening processes are completed.

ii. Ensuring that any related monetary transactions, management of client money, trust related activities are carried out only after appropriate sanctions screening processes are completed.

4.10. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

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

i. The "ISIL (Da'esh) &Al-Qaida Sanctions List", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

ii. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://www.un.org/securitycouncil/sanctions/1988/materials

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

4.10.3 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.

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

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

4.11.1 REs shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India.

4.11.2 In accordance with paragraph 3 of the aforementioned Order, REs shall ensure

not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

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

4.11.4 In case of match in the above cases, REs shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

4.11.5 REs may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

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

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

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

4.11.9 REs 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

4.11.10 In addition to the above, REs 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.

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

i. FATF Statements circulated in publicly domain for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. REs 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

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

Explanation: The processes referred to in (i) & (ii) above do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

iii. 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 relevant authorities, on request. REs are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

5. *Transaction Monitoring & Reporting of Suspicious Transactions to FIU-IND*

5.1.1 REs carrying out activities as notified under "The Notification" would be required to monitor the transactions carried out on behalf of their clients, or by their clients in the course of engaging in the notified activities. The transaction monitoring should also include counterparties to these transactions. They are also required to develop, implement, and maintain effective transactional monitoring systems to enable detection of possible ML/TF/PF activities. RE

may incorporate IP address tracking or digital footprint analysis for clients who primarily interact with it via digital/correspondence addresses.

5.1.2 REs are mandated to keep records of the alerts generated based on the Red Flag Indicators issued by FIU and keep records of the action taken on these Alerts.

5.1.3 REs carrying out transactions as notified under "The Notification" are required to, where they have reasonable grounds to suspect that funds are connected to any criminal activity or where the proceeds of crime or are related to ML, TF and PF, report their suspicions promptly to FIU-IND in a manner prescribed by FIU-IND.

5.1.4 Rule 8(2) read with Rule 3(1)(D) of the PMLR provides for prompt reporting of a suspicious transaction, which includes an attempted suspicious transaction, to the Financial Intelligence Unit (FIU-IND), if a reporting entity suspects or has reasonable grounds to suspect that funds used by a client are the proceeds of a criminal activity, or are related to terrorist financing. As detailed in Rule 3(1) of PMLR, suspicious transactions shall be reported promptly on forming of suspicion.

5.1.5 Suspicious activity monitoring program should be appropriate to REs carrying out transactions as notified under "The Notification" and the services they provide. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents/ office records/ memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Officer for recording their findings.

5.1.6 Nothing in these Regulations is intended to limit any function or power conferred on another body or authority under the AML/CFT/CPF laws.

6 Confidentiality.

RE, its Directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in PML Rules and furnishing of information to the Director is kept confidential. The records referred to PML Rules shall be maintained for a period of ten years from the date of cessation of the transactions between the clients and RE.

7 Prohibition on Tipping-off

Reporting entities and their directors, officers, and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") that an STR or related information is being considered, reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level. It is clarified that the reporting entities, irrespective of the amount of transaction and/or the threshold limit envisaged for reporting under PMLA, shall file an STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

8 Maintenance of Records

REs carrying out activities as notified under "The Notification" are required to maintain records of documents evidencing identity of their clients and beneficial owners as well as account files and business correspondence relating to their clients, for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later. Further, records of information relating to client transactions shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

9 Risk Assessment

9.1 REs shall carry out 'Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering, terrorist financing risk and proliferation financing risk.

9.2 Risk assessments must be designed and implemented to better understand risk exposure and areas in which there should be priority allocation of resources for appropriate control and oversight of their AML/CFT/CPF activities.

9.3 Reporting Entities carrying out activities as notified under "The Notification" shall carry out a risk assessment to identify, assess and take effective measures to mitigate its money laundering, terrorist financing and proliferation financing risk, severally and together, for customers, countries or geographic areas, and services, transactions or delivery channels to understand their risk exposure and ways to mitigate their money laundering and terrorist financing risk based on three main

categories Country/geographic risk, customer/counter-party risk, and product/service risk.

9.4 The periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the RE to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

9.5 A key element of their risk assessments will entail that they should Identify areas where their products/services could be exposed to ML/TF/PF risks e.g. identifying ML/TF risks facing a firm, given its clients, services, countries of operation, also having regard to publicly available information regarding ML/TF/PF risks; Customers carrying out extremely complex or high value transactions.

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

9.7 REs shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. REs shall implement a CDD programme, having regard to the ML/TF/PF risks identified and the size of business. Further, REs shall monitor the implementation of the controls and enhance them if necessary.

9.8 Risk assessment shall be followed by appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures, and controls.

9.9 The risk assessment shall be documented and be kept up-to-date. REs carrying out transactions as notified under “The Notification” 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, as and when required.

9.10 **Risk Categorisation of clients** : Certain clients may be of a higher, medium or lower risk category depending on the client’s background, type of business relationship or transaction, etc. In order to identify the types of clients that are likely to pose a higher- than-average risk of ML, TF or PF, REs carrying out activities as notified under “The Notification” shall develop appropriate client acceptance policies and procedures.

9.11 The risk assessment shall be documented and shall be made available to the Director, FIU-IND, as and when required. The following safeguards are to be followed while accepting the clients:

a) No reporting entity shall allow client engagement or availment of notified services under fictitious names or accounts on behalf of other persons whose identity has not been disclosed or cannot be verified.
b) The clients should be categorised in three categories, viz. high risk, medium risk and low risk.
c) Factors of risk perception for monitoring suspicious transactions of the clients are clearly defined having regard to clients' location, nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken.

9.12 A risk assessment of clients who are non-residents, high net worth individuals, trusts, PEPs, charities, NGOs, and organisations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners etc. will determine their ML/TF/PF risk.

9.13 In cases, where the identity of a client is ascertained as having a criminal background, a suspicious transaction report shall be filed with FIU-IND.

10. Access to Information under Section 12A of PMLA

10.1 Section 12A of the PMLA empowers the Director, FIU-IND to call for any information from the reporting entities as he considers necessary for the purposes of the PMLA and the reporting entities are required to furnish such information within such time and such manner as is specified by FIU-IND. Reporting entities are required to keep the information sought by the Director confidential.

10.2 The RE must ensure that adequate safeguards 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. 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;

10.3 The RE must establish standard transmission and encryption formats and

non- repudiation safeguards for electronic communication of data.

10.4 The RE must implement specific procedures for retaining internal records of transactions both domestic or international, 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 transactions involved, so as to provide, if necessary, evidence for prosecution of criminal activity.

10.5 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 where practicable, REs are required to seek and retain relevant identification documents for all such transactions and to report such transactions of suspicious funds.

11. Tracking regular updates through FINnet and Website

The PMLA and the PML Rules require every reporting entity to furnish prescribed transactions/reports, including suspicious transaction report (STR) to FIU-IND. The reports are to be furnished through the FINnet gateway portal (FINgate). FIU-IND website www.fiuindia.gov.in and www.fingate.gov.in, should be referred to for detailed guidance regarding registration and filing of reports. Detailed FAQs, periodic AML/CFT guidance and other related communication are also available in the website along with other relevant user guides. Further, updates for sanction screening lists as mentioned in these guidelines is also available on FIU-IND website

***