भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

सेबी/एच ओ/आईटीडी/आईटीडी_वीएपीटी/पी/सीआईआर/2023/032
SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/032 *February 22, 2023*

प्रति / To,

सभी स्टॉक एक्सचेंज / All Stock Exchanges
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन) / All Clearing Corporations
सभी निक्षेपागार (डिपॉज़िटरी) / All Depositories
सभी स्टॉक दलाल - एक्सचेंजों के जरिए / All Stock Brokers through Exchanges
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) - निक्षेपागारों (डिपॉज़िटरी) के जरिए
All Depository Participants through Depositories
सभी म्यूचुअल फंड / आस्ति प्रबंध कंपनियाँ (असेट मैनेजमेंट कंपनी) / न्यासी (ट्रस्टी) कंपनियाँ / म्यूचुअल फंडों के न्यासी मंडल / एएमएफआई / All Mutual Funds / Asset Management Companies / Trustee Companies / Boards of Trustees of Mutual Funds / Association of Mutual Funds in India (AMFI)
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ / All KYC Registration Agencies
सभी अर्हित निर्गम रजिस्ट्रार (रजिस्ट्रार टू एन इश्यू) / शेयर अंतरण अभिकर्ता (शेयर ट्रांसफर एजेंट)
All Qualified Registrars to an Issue / Share Transfer Agents

महोदय / महोदया,
Dear Sir / Madam,

विषयः साइबर सुरक्षा हेतु बेहतरीन पद्धतियाँ अपनाए जाने के संबंध में सेबी द्वारा विनियमित (रेग्यूलेटेड) एंटिटियों के लिए एडवाइज़री

Sub: Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices

1. यह देखने में आया है कि वित्तीय क्षेत्र के संगठन, स्टॉक एक्सचेंज, निक्षेपागार (डिपॉज़िटरी), म्यूचुअल फंड और वित्तीय क्षेत्र की अन्य एंटिटियाँ साइबर हमलों की समस्याओं से जूझ रही हैं और साथ ही इन हमलों की तादाद तेजी से बढ़ रही है और

1. Financial sector organizations, stock exchanges, depositories, mutual funds and other financial entities have been experiencing cyber incidents which are rapidly growing in frequency and sophistication.

जिनके नए-नए हथकंडे अपनाए जा रहे हैं । चूंकि वित्तीय एंटिटियों का कामकाज किसी न किसी रूप में या तो एक दूसरे से जुड़ा हुआ है या फिर एक दूसरे पर निर्भर रहता है, यही वजह है कि साइबर हमलों का खतरा आखिरकार किसी एक एंटिटी के सिस्टम (जिनमें वे सिस्टम भी शामिल हैं जिन पर उसका नियंत्रण हो), नेटवर्क आदि पर ही नहीं मंडराता, बल्कि इसका असर तो दूसरी एंटिटियों के सिस्टम, नेटवर्क आदि पर भी पड़ता है ।

Considering the interconnectedness and interdependency of the financial entities to carry out their functions, the cyber risk of any given entity is no longer limited to the entity's owned or controlled systems, networks and assets

2. यही नहीं, बल्कि साइबर हमले करने वाले जिस तरह पूरी साँठगाँठ करके साइबर हमले करने के लिए नए-नए हथकंडे अपनाते जा रहे हैं, उसके चलते अब हमें यह मानना ही होगा कि जोखिम को कम करने (रिस्क मैनेजमेंट) के लिए और संचालन (गवर्नेंस) को सुनिश्चित करने के लिए अब तक जो-जो तौर-तरीके अपनाए जाते थे, वे आज के माहौल में अब शायद इतने कारगर नहीं रहे कि नए-नए पैंतरे अपनाकर आज किए जा रहे साइबर हमलों से निपट पाएँ और न ही इतने कारगर रहे हैं कि सार्वजनिक क्षेत्र की तथा निजी क्षेत्र की कंपनियों में तकनीक की दिशा में हो रहे बदलावों के साथ कदम से कदम मिलाकर चल पाएँ ।

2. Further, given the sophistication and persistence of the threat with a high level of coordination among threat actors, it is important to recognize that many traditional approaches to risk management and governance that worked in the past may not be comprehensive or agile enough to address the rapid changes in the threat environment and the pace of technological change that is redefining public and private enterprise.

3. इसलिए, विनियमित एंटिटियों के लिए यह जरूरी है कि वे साइबर हमलों पर न केवल कारगर ढंग से काबू पाएँ, बल्कि सिस्टम को सामान्य स्थिति में भी लाएँ, ताकि ऐसे हमलों की वजह से वित्तीय स्थिरता पर आँच न आए।

3. Thus, an efficient and effective response to and recovery from a cyber-incident by REs are essential to limit any related financial stability risks. For ensuring the same,

यही सुनिश्चित करने के लिए, 'फाइनेंशियल कंप्यूटर सिक्यूरिटी इंसिडेंट रिस्पॉन्स टीम' ने सेबी के पास प्रस्तुत की गई अपनी रिपोर्ट में अपने अहम सुझाव दिए हैं । इस प्रकार जो भी सुझाव लागू हैं, वे इस परिपत्र (सर्कुलर) के साथ "संलग्नक-क" में एडवाइज़री के रूप में संलग्न हैं ।

Financial Computer Security Incident Response Team (CSIRT-Fin) has provided important recommendations in its report sent to SEBI. The applicable recommendations, in the form of an advisory, are enclosed at *Annexure-A* of this circular.

4. इस एडवाइज़री के साथ-साथ सेबी के लागू परिपत्रों (जिनमें साइबर सुरक्षा तथा साइबर आघात सहने संबंधी ढाँचा, वार्षिक सिस्टम ऑडिट संबंधी ढाँचा, आदि विषयों पर जारी किए गए परिपत्र भी शामिल हैं) और उसके बाद सेबी द्वारा समय-समय पर दी जाने वाली सूचनाओं आदि (अपडेट) पर भी अवश्य गौर किया जाए ।

4. This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework, Annual System Audit framework, etc.) and subsequent updates issued by SEBI from time to time.

5. विनियमित (रेग्यूलेटेड) एंटिटियाँ अपनी साइबर सुरक्षा की ऑडिट रिपोर्ट (यह ऑडिट साइबर सुरक्षा और साइबर आघात सहने के संबंध में सेबी द्वारा निर्धारित किए गए ढाँचे के अनुसार किया गया हो) के साथ इस एडवाइज़री का पालन किए जाने के संबंध में भी रिपोर्ट प्रस्तुत करेंगी । यह रिपोर्ट रिपोर्टिंग की मौजूदा व्यवस्था के अनुसार प्रस्तुत की जाएगी और यह रिपोर्ट साइबर सुरक्षा की ऑडिट रिपोर्ट प्रस्तुत करते समय प्रस्तुत की जाएगी ।

5. The compliance of the advisory shall be provided by the REs along with their cybersecurity audit report (conducted as per the applicable SEBI Cybersecurity and Cyber Resilience framework). The compliance shall be submitted as per the existing reporting mechanism and frequency of the respective cybersecurity audit.

6. इस परिपत्र के साथ संलग्न एडवाइज़री तुरंत प्रभाव से लागू होगी ।

6. The advisory annexed with this circular shall be effective with immediate effect.

7. यह परिपत्र (सर्कुलर) प्रतिभूतियों (सिक्यूरिटीज़) में निवेश करने वाले निवेशकों के हितों का संरक्षण करने, प्रतिभूति बाजार (सिक्यूरिटीज़ मार्केट) के विकास को बढ़ावा देने तथा उसे विनियमित (रेग्यूलेट) करने की दिशा में, भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 1992 की धारा 11(1) के तहत प्रदान की गई शक्तियों का प्रयोग करते हुए जारी किया जा रहा है ।

7. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

भवदीय / Yours Faithfully,

श्वेता बनर्जी Shweta Banerjee
उप महाप्रबंधक Deputy General Manager
दूरभाष / Phone: 022-26449509
ईमेल / Email: shwetas@sebi.gov.in

Annexure-A

In view of the increasing cybersecurity threat to the securities market, SEBI Regulated Entities (REs) are advised to implement the following practices as recommended by CSIRT-Fin:

1. **Roles and Responsibilities of Chief Information Security Officer (CISO)/ Designated Officer**:
   REs are advised to define roles and responsibilities of Chief Information Security Officer (CISO) and other senior personnel. Reporting and compliance requirements shall be clearly specified in the security policy.

2. **Measures against Phishing attacks/ websites**:
   i. The REs need to proactively monitor the cyberspace to identify phishing websites w.r.t. to REs domain and report the same to CSIRT-Fin/CERT-In for taking appropriate action.
   ii. Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense. Additionally, the advisories issued by CERT-In/ CSIRT-Fin may be referred for assistance in conducting exercises for public awareness.

3. **Patch Management and Vulnerability Assessment and Penetration Testing (VAPT):**
   i. All operating systems and applications should be updated with the latest patches on a regular basis. As an interim measure for zero-day vulnerabilities and where patches are not available, virtual patching can be considered for protecting systems and networks. This measure hinders cybercriminals from gaining access to any system through vulnerabilities in end-of-support and end-of-life applications and software. Patches should be sourced only from the authorized sites of the OEM.
   ii. Security audit / Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis and in accordance with the Cyber Security and Cyber Resilience circulars of SEBI issued from time to time.

The observation/ gaps of VAPT/Security Audit should be resolved as per the timelines prescribed by SEBI.

4. Measures for Data Protection and Data breach:

i. REs are advised to prepare detailed incident response plan.
ii. Enforce effective data protection, backup, and recovery measures.
iii. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data.
iv. Identify and classify sensitive and Personally Identifiable Information (PII) data and apply measures for encrypting such data in transit and at rest.
v. Deploy data leakage prevention (DLP) solutions / processes.

5. Log retention:

Strong log retention policy should be implemented as per extant SEBI regulations and required by CERT-In and IT Act 2000. REs are advised to audit that all logs are being collected. Monitoring of all logs of events and incidents to identify unusual patterns and behaviours should be done.

6. Password Policy/ Authentication Mechanisms:

i. Strong password policy should be implemented. The policy should include a clause of periodic review of accounts of ex-employees Passwords should not be reused across multiple accounts or list of passwords should not be stored on the system.
ii. Enable multi factor authentication (MFA) for all users that connect using online/internet facility and also particularly for virtual private networks, webmail and accounts that access critical systems.
iii. Maker and Checker framework should be implemented in strict manner and MFA should be enabled for all user accounts, especially for user accounts accessing critical applications.

7. Privilege Management:

i. Maker-Checker framework should be implemented for modifying the user's right in internal applications.
ii. For mitigating the insider threat problem, 'least privilege' approach to provide security for both on-and off-premises resources (i.e., zero-trust models) should

be implemented. Zero Trust is rooted in the principle of "trust nothing, verify everything." This security model requires strict identity verification for each and every resource and device attempting to get access to any information on a private network, regardless of where they are situated, within or outside of a network perimeter.

8. Cybersecurity Controls:

i. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses, block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

ii. Block the malicious domains/IPs after diligently verifying them without impacting the operations. CSIRT-Fin/CERT-In advisories which are published periodically should be referred for latest malicious domains/IPs, C&C DNS and links.

iii. Restrict execution of "powershell" and "wscript" in enterprise environment, if not required. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

iv. Utilize host based firewall to prevent Remote Procedure Call (RPC) and Server Message Block (SMB) communication among endpoints whenever possible. This limits lateral movement as well as other attack activities.

v. Practice of whitelisting of ports based on business usage at Firewall level should be implemented rather than blacklisting of certain ports. Traffic on all other ports which have not been whitelisted should be blocked by default.

9. Security of Cloud Services:

i. Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.

ii. Ensure proper security of cloud access tokens. The tokens should not be exposed publicly in website source code, any configuration files etc.

iii. Implement appropriate security measures for testing, staging and backup environments hosted on cloud. Ensure that production environment is kept properly segregated from these. Disable/remove older or testing environments if their usage is no longer required.

iv. Consider employing hybrid data security tools that focus on operating in a shared responsibility model for cloud-based environments.

10. Implementation of CERT-In/ CSIRT-Fin Advisories:

The advisories issued by CERT-In should be implemented in letter and spirit by the regulated entities. Additionally, the advisories should be implemented promptly as and when received.

11. Concentration Risk on Outsourced Agencies:

i. It has been observed that single third party vendors are providing services to multiple REs, which creates concentration risk. Here, such third parties though being small non-financial organizations, if any cyber-attack, happens at such organizations, the same could have systemic implication due to high concentration risk.

ii. Thus, there is a need for identification of such organizations and prescribing specific cyber security controls, including audit of their systems and protocols from independent auditors, to mitigate such concentration risk.

iii. Further, REs also need to take into account this concentration risk while outsourcing multiple critical services to the same vendor.

12. Audit and ISO Certification:

i. SEBI's instructions on external audit of REs by independent auditors empaneled by CERT-In should be complied with in letter and spirit.

ii. The REs are also advised to go for ISO certification as the same provides a reasonable assurance on the preparedness of the RE with respect to cybersecurity.

iii. Due diligence with respect to audit process and tools used for such audit needs to be undertaken to ensure competence and effectiveness of audits.

भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

MASTER CIRCULAR

SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 **June 06, 2024**

To,

1. **All Intermediaries registered with SEBI under Section 12 of the Securities and Exchange Board of India Act, 1992**
2. **Stock Exchanges**

Dear Sir/Madam,

Subject: Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under.

1. The Prevention of Money Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules[1]), as amended from time to time and notified by the Government of India, mandate every reporting entity [which includes intermediaries registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) and stock exchanges], to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities. The PML Rules, inter alia, empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by the regulator.

2. The enclosed guidelines stipulate the essential principles for combating Money Laundering (ML) and Terrorist Financing (TF) and provide detailed procedures and obligations to be followed and complied with by all the registered intermediaries.

[1] https://fiuindia.gov.in/files/AML_Legislation/notification.html

3. These guidelines shall also apply to the branches of the Stock Exchanges, registered intermediaries, and their subsidiaries situated abroad, especially, in countries which do not apply or insufficiently apply the recommendations made by the Financial Action Task Force (FATF), to the extent local laws and regulations permit. When the local applicable laws and regulations prohibit implementation of these requirements, the same shall be brought to the notice of SEBI.

4. SEBI has from time to time issued circulars/directives with regard to Know Your Client (KYC), Client Due Diligence (CDD), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) specifying the minimum requirements. It is emphasized that the registered intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address the concerns of money laundering and suspicious transactions undertaken by clients.

5. On and from the issue of this Circular, the earlier circulars issued by SEBI on the subject of Anti-Money Laundering and Combating the Financing of Terrorism, listed out in the Appendix, shall stand rescinded. Notwithstanding such rescission, anything done or any action taken or purported to have been done or taken under the circulars specified in Appendix, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular.

6. This Master Circular shall supersede the previous Master Circular reference no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 and is available at www.sebi.gov.in under the link “Legal ⟹ Master Circulars”.

Yours faithfully,

Sapna Sinha
Deputy General Manager
Phone No. 022-26449748
Email id: sapnas@sebi.gov.in

Table of Contents

Overview

1. The Directives as outlined below provide a general background and summary of the main provisions of the applicable anti-money laundering and anti-terrorist financing legislations in India. They also provide guidance on the practical implications of the Prevention of Money Laundering Act, 2002 (**PMLA**). The Directives also set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities.

2. These Directives are intended for use primarily by intermediaries registered under Section 12 of the Securities and Exchange Board of India Act, 1992 **(SEBI Act),** Stock Exchanges, Depositories and other recognised entities under the SEBI Act and Regulations and rules thereunder**.** While it is recognized that a "one-size-fits-all" approach may not be appropriate for the securities industry in India, each registered intermediary shall consider the specific nature of its business, organizational structure, type of clients and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

Background

3. As per the provisions of PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time and notified by the Government of India, every reporting entity (which includes intermediaries registered under section 12 of the SEBI Act, i.e. a stock-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the SEBI Act and stock exchanges), shall have to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

The PML Rules empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by the regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by SEBI.

4. The PMLA inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as provided in Section 12A read with Section 24 of the SEBI Act will be treated as a scheduled offence under schedule B of the PMLA.

Policies and Procedures to Combat Money Laundering and Terrorist Financing

Essential Principles:

5. These Directives have taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed directives have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

6. In case there is a variance in Client Due Diligence (CDD)/ Anti Money Laundering (AML) standards specified by SEBI and the regulators of the host country, branches/overseas subsidiaries of registered intermediaries are required to adopt the more stringent requirements of the two.

7. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform SEBI.

Obligation to establish policies and procedures

8. Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all registered intermediaries ensure the fulfilment of the aforementioned obligations.

9. The term “group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of Rule 2 of the PML Rules as amended from time to time. Groups shall implement group-wide policies for the purpose of discharging obligations under Chapter IV of the PMLA.

10. Financial groups shall be required to implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group as under:
    a. policies and procedures for sharing information required for the purposes of CDD 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 shall include information and analysis of transactions or activities which appear unusual (if such analysis was done);

       similar provisions for receipt of such information by branches and subsidiaries 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.

11. To be in compliance with these obligations, the senior management of a registered intermediary 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 registered intermediaries shall:

i. issue a statement of policies and procedures and implement, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;

ii. ensure that the content of these Directives are understood by all staff members;

iii. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;

iv. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;

v. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

vi. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

vii. develop staff members' awareness and vigilance to guard against ML and TF.

12. Policies and procedures to combat ML and TF shall cover:

i. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities

transactions, money and client records etc. whether in branches, departments or subsidiaries;

ii. Client acceptance policy and client due diligence measures, including requirements for proper identification;

iii. Maintenance of records;

iv. Compliance with relevant statutory and regulatory requirements;

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

vi. 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 front line staff, of their responsibilities in this regard; and,

vii. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

Written Anti Money Laundering Procedures

13. Each registered intermediary shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following four specific parameters which are related to the overall 'Client Due Diligence Process':

    i. Policy for acceptance of clients;
    ii. Procedure for identifying the clients;
    iii. Risk Management;
    iv. Monitoring of Transactions.

Client Due Diligence (CDD)

14. Client Due Diligence means due diligence carried out on a client referred to in clause (ha) of sub-section (1) of section 2 of the PMLA using reliable and independent sources of identification.

15. The CDD shall have regard to the money laundering and terrorist financing risks and the size of the business and shall include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the registered intermediary or through national risk assessment.

16. The CDD measures comprise the following:

    i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using reliable and independent client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;

    ii. Identify the clients, verify their identity using reliable and independent sources of identification, obtain information on the purpose and intended nature of the business relationship, where applicable;

    iii. Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person;

    Provided that in case of a Trust, the reporting entity shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

iv. Identifying beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted. The beneficial owner shall be determined as under-

a) **where the client is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

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

i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of 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 client 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 ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation:- For the purpose of this clause:-

"Control" shall include the right to control the management or policy decision;

c) **where the client 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 ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;

d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e) **Where the client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust, settlor, protector and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or 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.

g) **Applicability for foreign investors**: Registered intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client;

h) The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

v. Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (iii);

vi. Understand the nature of business, ownership and control structure of the client;

vii. Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

viii. Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data.

ix. Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

x. Every registered intermediary shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

xi. Where registered intermediary is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND.

17. No transaction or account-based relationship shall be undertaken without following the CDD procedure.

Policy for acceptance of clients

18. All registered intermediaries shall develop client acceptance policies and procedures that aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, they will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients:

i. No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified;

ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile;

iii. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

a) Non - resident clients;
b) High net-worth clients;
c) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations;
d) Companies having close family shareholdings or beneficial ownership;
e) Politically Exposed Persons" (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the PML Rules. The additional

norms applicable to PEP as contained in the subsequent paragraph 20 of the master circular shall also be applied to the accounts of the family members or close relatives / associates of PEPs;

f) Clients in high risk countries. While dealing with clients from or situated in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspected, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situated in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. The intermediary shall specifically apply EDD measures, 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;

g) Non face to face clients - Non face to face clients means clients who open accounts without visiting the branches/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients;

h) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

iv. Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and

having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

v. Ensure that an account is not opened where the intermediary is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non - co-operation of the client in providing full and complete information. The registered intermediary shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The registered intermediary shall be cautious to ensure that it does not return securities or money that may be from suspicious trades. However, the registered intermediary shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

vi. The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons i.e. the agent-client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

vii. Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

viii. The CDD process shall necessarily be revisited when there are suspicions of ML/TF.

Client identification procedure

19. The KYC policy shall clearly spell out the client identification procedure (CIP) to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

20. Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP**:**

i. All registered intermediaries shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.

ii. All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

iii. Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

iv. The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.

vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

21. SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time, all registered intermediaries shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

22. Further, the intermediary shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing.

23. Every intermediary shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

    It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to registered intermediaries (brokers, depository participants, AMCs etc.) from obtaining the minimum information/documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly

implemented by all registered intermediaries and non-compliance shall attract appropriate sanctions.

Reliance on third party for carrying out Client Due Diligence (CDD)

24. Registered intermediaries may rely on a third party for the purpose of -

i. identification and verification of the identity of a client and

ii. Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

25. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules:

i. The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;

ii. The registered intermediary shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

iii. The registered intermediary shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

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

v. The registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

Risk Management

Risk-based Approach

26. Registered intermediaries shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, the registered intermediaries shall monitor the implementation of the controls and enhance them if necessary.

27. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

28. Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

Risk Assessment

29. Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

30. The risk assessment carried out 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. The assessment shall be documented, updated

regularly and made available to competent authorities and self-regulating bodies, as and when required.

31. The Stock Exchanges and registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries 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.

32. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

Monitoring of Transactions

33. Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities.

34. The intermediary shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client 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 SEBI/stock exchanges/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

35. The registered intermediaries shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

36. The intermediary shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the intermediary.

37. Further, the compliance cell of the intermediary shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

Suspicious Transaction Monitoring and Reporting

38. Registered Intermediaries shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

39. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

    i Clients whose identity verification seems difficult or clients that appear not to cooperate;

    ii Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;

iii Clients based in high risk jurisdictions;

iv Substantial increases in business without apparent cause;

v Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

vi Attempted transfer of investment proceeds to apparently unrelated third parties;

vii Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

40. Any suspicious transaction shall be immediately notified to the **Designated/Principal Officer** within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

41. It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

42. Paragraph 18 (iii) (f) of this Circular categorizes clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. Registered intermediaries are directed that such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting

mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

Record Management

Information to be maintained

43. Registered Intermediaries are required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

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

Record Keeping

44. Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

45. Registered Intermediaries shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

46. In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

    i. the beneficial owner of the account;
    ii. the volume of the funds flowing through the account; and
    iii. for selected transactions:
        a. the origin of the funds

b. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
c. the identity of the person undertaking the transaction;
d. the destination of the funds;
e. the form of instruction and authority.

47. Registered Intermediaries shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

48. More specifically, all the registered intermediaries shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

ii. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.

iii. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

iv. all suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such

as demat account, security account maintained by the registered intermediary.

49. Where the registered entity does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

Retention of Records

50. Registered intermediaries shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.

51. As stated in paragraph 19 and 20, registered intermediaries are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

52. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

53. Registered Intermediaries shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are

reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

Procedure for freezing of funds, financial assets or economic resources or related services

54. The Stock exchanges and the registered intermediaries shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any accounts 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).

55. In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2). Corrigendums dated March 15, 2023 and April 22, 2024 have also been issued in this regard (Annexure 3) and (Annexure 4). The list of Nodal Officers for UAPA is available on the website of MHA.

Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries

56. The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.

57. In terms of Section 12A of the WMD Act, the Central Government is empowered as under:

"(2) For prevention of financing by any person of any activity which is prohibited under the WMD 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 the WMD 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."

58. The stock exchanges and registered intermediaries are directed to comply with the procedure laid down in the said Order.

59. The stock exchanges and registered intermediaries shall:

(i) Maintain the list of individuals/entities ("**Designated List"**) and update it, without delay, in terms of paragraph 2.1 of the Order;

(ii) verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries 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 Central Nodal Officer ("CNO"), without delay. The details of the CNO are as under:

The Director
FIU-INDIA
Tel.No.:011-23314458, 011-23314459 (FAX)
Email: dir@fiuindia.gov.in

(iii) run a check, on the given parameters, at the time of establishing a relation with a client 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 clients' particulars match with the particulars of Designated List, stock exchanges and registered intermediaries 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, without delay;

(iv) send a copy of the communication, mentioned in paragraphs 59(ii) and 59(iii) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051;

(v) prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall

under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act;

(vi) file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs 59(ii) and (iii) above, carried through or attempted through.

60. Upon the receipt of the information above, the CNO would cause a verification to be conducted by the appropriate authorities to ensure that the individuals/entities identified are the ones in the Designated List and the funds, financial assets or economic resources or related services, reported are in respect of the designated individuals/entities. 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 and be conveyed to the concerned reporting entity 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.

61. Reporting entities shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of Designated Individuals/ Entities

62. The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The registered intermediaries shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

63. All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

64. An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at https://press.un.org/en/content/press-release. The details of the 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://www.un.org/securitycouncil/sanctions/1267/press-releases ;
ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

65. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

66. The Stock Exchanges and the registered intermediaries shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

67. The Stock Exchanges and the registered intermediaries shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

68. The Stock exchanges and the registered intermediaries shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions

carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

69. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

70. The Stock exchanges and the registered intermediaries shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

71. FATF Secretariat after conclusion of each of it's plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the registered intermediaries.

72. The registered intermediaries shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not

precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

Reporting to Financial Intelligence Unit-India

73. In terms of the PML Rules, registered intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit - India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone : 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email:helpdesk@fiuindia.gov.in
(For FINnet and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity / Principal Officer registration related queries)
complaints@fiuindia.gov.in
Website: http://fiuindia.gov.in

74. Registered intermediaries shall carefully go through all the reporting requirements (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Brochures on FIU_p.pdf) and formats that are available on the website of FIU – IND under the Section Home - FINNET 2.0 – User Manuals and Guides -Reporting Format (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Reporting_Format_p.pdf). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND.

The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, registered intermediaries shall adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month;

ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion;

iii. The Non Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month;

iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND;

vi. No NIL reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported;

vii. "Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

viii. Every registered intermediary, its Directors, officers and all employees shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential.

Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

75. Registered Intermediaries shall not put any restrictions on operations in the accounts where an STR has been made. Registered intermediaries and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being 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 registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

    It is further clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

    Confidentiality requirement does not inhibit information sharing among entities in the group.

Designation of officers for ensuring compliance with provisions of PMLA

76. **Appointment of a Principal Officer:** To ensure that the registered intermediaries properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary;
Provided that such officer shall be an officer at the management level.

77. **Appointment of a Designated Director**: In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

"Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,

b) the managing partner if the reporting entity is a partnership firm,

c) the proprietor if the reporting entity is a proprietorship firm,

d) the managing trustee if the reporting entity is a trust,

e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above".

78. In terms of Section 13 (2) of the PMLA, the Director, FIU – IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

79. Registered intermediaries shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

Hiring and Training of Employees and Investor Education

80. Hiring of Employees: The registered intermediaries shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

81. Training of Employees: The registered intermediaries shall have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

82. Investor Education: Implementation of AML/CFT measures requires registered intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. There is, therefore, a need for registered intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Registered intermediaries shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

Repeal and Savings

83. On and from the issue of this Circular, the circulars listed out in the Appendix to this Circular shall stand rescinded. Notwithstanding such rescission, anything done or any action taken or purported to have been done or taken, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular.

Appendix

The following Circulars shall stand rescinded from the date of issuance of this Circular

1. **SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June 16, 2023 -** Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

2. **SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/0170 dated October 13, 2023 -** Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

3. **SEBI/HO/MIRSD/SEC-5/P/CIR/2023/062 dated April 26, 2023 -** Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries.

4. **SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 –** Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under.