

PMLA POLICY

Of

CNB Finwiz Private Limited being the member of NSE/BSE/MCX Ltd vide SEBI Reg. No. INZ000204238 and DP of CDSL vide SEBI Reg. No. IN-DP-570-2021

Policy Version No.:1.4

Date of Last Review: 19 Aug, 2024

Placed in Board Meeting dated: 19 Aug, 2024

Circular Ref: SEBI Master circular SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated 3rd Feb, 2023, SEBI, SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 and SEBI/HO/MIRSD/SECFATF/P/CIR/2023/0170 and SEBI/HO/MIRSD/SECFATF/P/CIR/2024/78 dated 06 June 2024.

Prepared by: Mr. Parvender Singh/Ram Niwas

Reviewed by: Mr. Paras Sharma

POLICY FRAMEWORK FOR IMPLEMENTATION OF THE PROVISIONS OF PREVENTION AND MONEY LAUNDERING ACT (PMLA) 2002

INTRODUCTION

The Prevention of Money Laundering Act, 2002 (**PMLA**) came in force with effect from 1st July 2005.

As per the provisions of the PMLA, each market intermediary (**Reporting Entity**) (which includes a stockbroker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the Securities and Exchange Board of India Act, 1992 (**SEBI Act**)) shall have to adhere to client account opening procedures and maintain records of such "transactions" as prescribed by the PMLA and Rules notified there under.

Obligations of a "Reporting Entity" includes:-

- a. to maintain a record of all transactions covered as per the nature and value of which may be prescribed, in such manner as to enable it to reconstruct individual transactions
- b. furnish to the Partner (FIU) within such time as may be prescribed information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed
- c. verify the identity of its clients in such manner and subject to such conditions as may be prescribed
- d. identify the beneficial owner, if any, of such of its clients, as may be prescribed
- e. Maintain record of documents evidencing identity of its clients and beneficial owners, account files and business correspondence relating to its clients and information related to transactions for specified period.

For the purpose of PMLA, transactions include:

1. all cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency.
2. all series of cash transactions integrally connected to each other, which have been valued below Rs.10 Lakhs or its equivalent in foreign currency, such series of transactions within one calendar month.
3. all suspicious transactions (remotely / integrally connected or related), whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as Demat account, security account maintained by the registered intermediary.

Further, In case there is a variance in CDD/AML standards prescribed by SEBI and the regulators of the host country, branches/overseas subsidiaries of intermediaries are required to adopt the more stringent requirements of the two.

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.

For the purpose "**Suspicious Transaction**" means a transaction whether or not made in cash which to a person acting in good faith:-

- a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to have no economic rationale or bona fide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

The Anti-Money Laundering Guidelines provides a general background on the subjects of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to identify and discourage any "Money Laundering" (ML) or "Terrorist Financing" activities.

SEBI has issued various directives vide circulars, from time to time, covering issues related to Know Your Client (**KYC**) norms, Anti- Money Laundering (**AML**), Client Due Diligence (**CDD**) and Combating Financing of Terrorism (**CFT**). The directives lay down the minimum requirements and it is emphasized that the intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

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 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.

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 Term "group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of Rule 2 of the PMLA 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.

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.

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 obligations of an intermediary under Prevention of Money Laundering Act, 2002 (PLMA) includes:-

- a. 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;
- b. ensure that the content of these Directives are understood by all staff members;
- c. 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;
- d. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
- e. 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;
- f. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
- g. develop staff members' awareness and vigilance to guard against ML and TF.

The Policies and procedures to combat ML and TF shall cover:

- a. 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;
- b. Client acceptance policy and client due diligence measures, including requirements for proper identification;
- c. Maintenance of records;
- d. Compliance with relevant statutory and regulatory requirements;
- e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
- f. 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,
- g. 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.

Accordingly, we have drafted this written policy framework (hereinafter called as "PMLA Policy") which aims to have a system in place to identify, monitor and reporting the suspected money laundering or terrorist financing transactions to law enforcing authorities within the framework of current statutory and regulatory requirements.

This policy includes the following four specific parameters which are related to the overall 'Client Due Diligence Process':

- a. Policy for acceptance of clients;
- b. Procedure for identifying the clients;
- c. Risk Management;
- d. Monitoring of Transactions.

All concerned are hereby advised to ensure that every possible measures are taken for the effective implementation of this Policy and that the measures taken are adequate, appropriate and abide by the spirit and requirements as enshrined in the PMLA.

Detailed PMLA Policy Framework

1. 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.

Complete Details of Principle are as given below:-

Name: Paras Sharma
Designation: Principal Officer
Contact No :8860078514
Email:cs@cnbfinwiz.com

Rights and Obligations of Principle Officer:

- a. The principal office shall have all time access to customer identification data and other CDD information.
- b. The principal officer shall have complete independence and authority to access and is able to report to Senior Management or his/her next reporting level or the Board of Directors.

Responsibilities:

The Principal Officer shall ensure that:

- a. the Board approved PMLA Policy framework is implemented effectively.
- b. systems generated data based on set parameters is regularly and promptly downloaded to analyze, identify and report transactions of suspicious nature to FIU-IND directly
- c. group responds promptly to any request for information, including KYC related information maintained by us, made by the regulators, FIU-IND and other statutory authorities.
- d. group's staff members and associates are trained to address issues related to the application of the PMLA.
- e. the staff selection and training process complies with the PMLA Policy.
- f. group and all concerned staff is regularly updated regarding any changes / additions / modifications in PMLA provisions.

2. Appointment of Designated Director

For ensuring overall supervision and compliance with the obligations imposed under chapter IV of the Act and the Rules the group has appointed the "Designated Director". The details of the designated Director are as given below:-

Name: Mr. Naman Bagri
Designation: Designated Director
Contact No :9873752222
Email: naman.bagri@cnbfinwiz.com

3. Client Due Diligence Measures (CDD Measures)

The CDD measures comprise the following:

- a. Obtain 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 client identification and verification procedures.

For this purpose, 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;”

- b. 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.
- c. 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, we 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, we shall ensure that trustees disclose their status at the time of commencement of an account based relationship.
- d. Identify 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;

Suggestive measures for identification of **beneficial ownership** are as given below:-

- i.) **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;
- ii.) **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;
- iii.) **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;
- iv.) where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
- v.) **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 and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
- vi.) 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.
- vii.) **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;
- viii.) 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.

- e. 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 (c);
- f. Understand the nature of business, ownership and control structure of the client;
- g. 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;
- h. 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; and
- i. 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.
- j. We 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 us has ended or the account has been closed, whichever is later.
- k. In case of any suspicious transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, We shall not pursue the CDD process, and shall instead file a STR with FIU-IND."
- l. No transaction or account-based relationship shall be undertaken without following the CDD procedure."

Reliance on third party for carrying out due diligence

We may rely on a third party for the purpose of

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

- b. where the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.

Provided such third party is regulated, supervised or monitored by SEBI, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

Such reliance shall however 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 e.g.

- a. we shall immediately obtain necessary information of such client due diligence carried out by the third party;
- b. we shall take adequate steps to satisfy ourself 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;
- c. we 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;
- d. The third party is not based in a country or jurisdiction assessed as high risk

It must always be ensured and kept in mind that as a registered intermediary, we shall be ultimately responsible for CDD and undertaking enhanced due diligence measures.

4. Policy for acceptance of Clients

Our client acceptance policies and procedures aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF so that we are in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transactions.

In nutshell the following safeguards are to be followed while accepting the clients namely;

- a. No account is opened in a fictitious / benami name or on an anonymous basis.
- b. Each client shall be classified into low or medium or high risk categories depending upon the risk perception.

Such risk categorization may be arrived considering various factors of risk perception of the client 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.

Clients of Special Category (CSC) (as defined later in this policy) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client (**KYC**) profile.

- c. 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.

We must obtain documentary evidence of each KYC information provided by the client and verify each such supporting document with originals prior to acceptance of a copy and same be stamped "Verified with the original" and each client must be met in person before registration.

The information collected by us should be enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines.

A complete identification record of person doing the In-person verification and verification of documents must be kept in readily available manner.

- d. We should not open an account where we are unable to apply appropriate CDD measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided by the client is suspected to be non-genuine, or there is perceived non co-operation of the client in providing full and complete information.

We shall not continue to do business with such a person and file a suspicious activity report. We shall also evaluate whether there is suspicious any trading in determining whether to freeze or close the account. We shall be cautious to ensure that we do not return securities or money that may be from suspicious trades.

Further, we shall consult the relevant authorities in determining what action we shall take when we suspects suspicious trading activity.

- e. We shall ensure that in case of individual client only the client himself/ herself be allowed to transact on his/her own behalf. A person may be allowed to deal on behalf of his / her spouse, dependent children or dependent parents provided a written authorization is obtained from concerned family member.

In case of non-individual clients only the person(s) having appropriate written authorization are allowed to deal for and on behalf of the client.

In all the cases, we must obtain the identification documents of the person so authorized to deal on behalf of the client and adequate verification of person's authority to act on behalf of the client shall also be carried out.

The authorization letter should specify the manner in which the account shall be operated, transaction limits for the operation, additional authority (if any) required for transactions exceeding a specified quantity/value.

- f. Before activating any account, we must 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.

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 <http://www.un.org>.

- g. The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

For the purpose of above and elsewhere used in this policy framework, Clients of Special Category (**CSC**) shall include:-

- i.) Non resident clients
- ii.) High net-worth clients
- iii.) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
- iv.) Companies having close family shareholdings or beneficial ownership
- v.) Politically Exposed Persons" (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. 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;
- vi.) Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements

that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information which they may have access to. However, this shall not preclude us 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.

We 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.

- vii.) Non face to face clients means clients who open accounts without visiting the branch/offices. Video based customer identification process is treated as face-to-face onboarding of clients
- viii.) Clients with dubious reputation as per public information available etc.

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

5. Client Identification Procedures:-

Client identification procedure shall be carried out at different stages i.e. while establishing the relationship with the client, while carrying out transactions for the client or when there is any doubt regarding the veracity or the adequacy of previously obtained client identification data.

In order to ensure the compliance, we must:-

- identify whether the client or potential client or the beneficial owner of such client is a politically exposed person.

In such cases we must seek relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.

- Senior management's prior approval is mandatory for establishing business relationships with PEPs. Further, where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, we shall obtain senior management approval to continue the business relationship.
- Reasonable measures shall be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

- The client shall be identified by obtaining adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- Client's information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the Senior Management.
- We must follow SEBI prescribed minimum requirements relating to KYC for certain classes of registered intermediaries from time to time and conduct ongoing due diligence where inconsistencies in the information provided by the client are noticed.
- Irrespective of the amount of investment made by clients, no minimum threshold or exemption is available 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 any client and non-compliance shall attract appropriate sanctions / regulatory actions.
- The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

6. Risk-Based Approach to KYC

Client acceptance is a critical activity in AML compliance. Registering any client means providing such client with an entry point to local and international financial systems. Client acceptance, thus, becomes the first step in controlling money laundering and terrorist financing.

Regulatory guidelines stipulate that a sound KYC program should determine the true identity and existence of the customer and the risk associated with the customer. It is therefore imperative that we capture information about their background, sources of funds, nature and type of business, domicile and financial products used by them and how these are delivered to them in order to properly understand their risk profile.

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. 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 we shall obtain necessarily depend on the risk category of a particular client and for this purpose clients may be classified into following categories namely;-

Category - A: Low Risk

Category - B: Medium Risk

Category - C: High Risk

Category "A" clients are those pose low or nil risk. These clients have a respectable and verifiable social and financial standing. Their KYC Information and financial details is easily verifiable.

Category "B" Clients are those who have suspicious background, in that case we deeply verify Background Details, Understand the Source of fund and wealth of the Customer and Beneficial Owners, Types of Business, Enhance Transaction Monitoring, Transactions and who maintain running account without making / withdrawing payment / deliveries frequently.

Category "C" Clients are those who have suspicious background as per above mentioned in medium risk clients category and who have defaulted in the past or the clients identified as CSC.

Further, low risk profile 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.

Any business relationship with "High Risk Clients" including clients identified as CSC must not be commenced unless approved by Senior Management Officials.

As customer risk rating and KYC drives enhanced due diligence and ongoing monitoring it is critical that an ongoing comprehensive assessment is conducted to understand the risks associated with our business and customers and necessary modifications and improvements in associated Client acceptance and Due Diligence Policies and Procedures are made.

Risk Assessment

We have formulated a periodic risk assessment mechanism to, identify money laundering and terrorist financing risk, assess and take effective measures to mitigate them with respect to our clients, countries or geographical areas, nature and volume of transactions, payment methods used by our clients, etc.

We 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. We shall also 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”.

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 (these can be accessed at the URL - http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>)

Our risk assessment process consider all the relevant factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied and assessment is documented and updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

7. Transaction based Monitoring and Identification of Suspicious Transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. We can effectively control and reduce the risk only if we have an understanding of the normal and reasonable activity of the client so that we can identify deviations in transactions.

However, the extent of monitoring will depend on the risk sensitivity of the account.

Special attention is required to be given to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. We have specified internal threshold limits for each class of client accounts and do regular monitoring of the transactions which exceeds these limits.

For the purpose of monitoring of transaction under PMLA following should be taken care of:

- a. examine the background and the purpose of transactions which are complex or unusually large/ with patterns which appear to have no economic purpose
- b. transactions which exceed the limits specified for the relevant class of client accounts
- c. understanding of normal activity in client account to identify deviations and substantial increase in business without any apparent cause
- d. clients transferring large sums of money to/from overseas locations
- e. attempted transfer of proceeds to unrelated 3rd parties
- f. transactions of clients based in high risk jurisdictions
- g. Unusual transactions by CSCs and businesses undertaken by offshore banks / financial services, businesses reported to be in the nature of export- import of small items
- h. Random examination of a selection of transaction to comment on their nature

Broad category of triggers that will require the complete analysis of transaction may include:-

- a. Transactions involving Artificial Volume Creation / High Value Deals / Synchronized Trades
- b. client's disproportionate volume with respect to his last known financial details
- c. scrip concentration-concentrated position in particular scrips which have an unusual price or volumes
- d. high value off market transfer instructions
- e. high value transactions in a new/dormant account
- f. frequent small quantity transactions in an account
- g. transaction undertaken by client with respect to whom alerts raised by employees/media reports/ Enforcement Agency etc.
- h. transactions undertaken by customers for whom there are adverse media reports about criminal activities/terrorist activities / terrorist financing activities
- i. transaction undertaken by customers who offered false/forged identification documents / address found to be wrong

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:-

- a. Clients whose identity verification seems difficult or clients that appear not to cooperate
- b. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
- c. Clients based in high risk jurisdictions;
- d. Substantial increases in business without apparent cause;
- e. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- f. Attempted transfer of investment proceeds to apparently unrelated third parties;
- g. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export- import of small items.

The background including all documents/office records /memorandums/clarifications sought pertaining to identified transactions and purpose thereof shall be examined carefully and findings shall be recorded in writing.

Findings of transaction analysis must be recorded in writing, as the same along with records and related documents may required to be provided to auditors, SEBI, Stock Exchanges, FIUIND, other relevant authorities during audits or as and when asked for.

We shall apply client due diligence measures to existing clients also 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.

The compliance cell 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.

These records are required to be maintained in terms of Section 12 of the PMLA be and preserved for a period of five years from the date of transaction with the client. The 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.

8. Reporting of Suspicious Transactions

The Principal Officer would act as a central reference point in playing an active role in the identification and assessment of potentially suspicious transactions and facilitating onward reporting of suspicious transactions.

Accordingly, any potential suspicious transaction shall immediately be notified to Principal Officer which may be a detailed report with specific reference to the clients, transactions and the nature / reason of suspicion and for this purpose, transactions abandoned or aborted by clients on being asked to give some details or to provide documents are also to be reported even if not completed by clients, irrespective of the amount of the transaction.

We must ensure continuity in dealing with the reported client as normal until told otherwise and the client not be told of the report/suspicion i.e. group officials and employees shall be prohibited from "Tipping off" the fact that a STR or related information is being reported or provided to the FIU-IND.

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 Principal Officer shall examine the transaction in details and if reaches to the conclusion that the notified transaction is "Suspicious" shall report the same to **Financial Intelligence Unit** (FIU) within 7 days from the date of arriving at such conclusion by filing the Suspicion Transaction Report (STR).

It is clarified that the STR must be filed irrespective of the amount of transaction and/or the threshold limit, if there are reasonable grounds to believe that the transactions involve proceeds of crime.

The 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, shall be categorised as 'CSC'. 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.

9. Information to be maintained

We shall 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

10. Record Keeping

We, as an SEBI registered Intermediary, shall maintain all the records to ensure compliance of requirements contained in SEBI Act 1992, Rules and Regulations made there under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

We are required to 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.

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:

- a. the beneficial owner of the account;
- b. the volume of the funds flowing through the account; and
- c. for selected transactions:
 - i. the origin of the funds
 - ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc
 - iii. the identity of the person undertaking the transaction;
 - iv. the destination of the funds;
 - v. the form of instruction and authority.

We 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, we 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.

We shall ensure maintaining proper record of transactions prescribed under Rule 3 of PML Rules) namely;-

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

- c. 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;
- d. 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

Records to be maintained in a way that all client and transaction records and information are available on a timely basis to the competent investigating authorities.

In case, we does not have records of the identity of its existing clients, then we shall obtain the records forthwith, failing which the we 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 Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

11. Retention of Records

We shall ensure Internal mechanism for proper maintenance and preservation of records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities

Following Document Retention Terms should be observed:

- a. the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of **FIVE YEARS (5)** from the date of transactions with the client.
- b. Records evidencing the identity of clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of **FIVE YEARS (5)** after the business relationship between a client has ended or the account has been closed, whichever is later
- c. In situations where the records relate to on-going investigation or transactions, which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.
- d. All necessary records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, shall be maintained and preserved for a period of **FIVE YEARS (5)** from the date of the transaction with the client.
- e. As per SEBI (D&P) Regulation No. SEBI/LAD-NRO/GN/2018/40 dated 03.10.2018, all necessary records of information are maintained and preserved for a minimum period of **YEARS (8)**.

Records may be maintained in both hard and / or soft copies.

12. List of Designated Individuals/Entities

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

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.

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.

We ensure that accounts are not opened in the name of anyone whose name appears in said list. We 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.

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

We shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

We 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.

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.

We 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 FATE, Market Company Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

13. Jurisdictions that do not or insufficiently apply the FATF

FATF Secretariat after conclusion of each of its 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 us.

We shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements.

14. Employees Hiring

We have adequate screening procedures in place to ensure high standard when hiring employees. We have identified the key positions within the Company structure having regard to the risk of money laundering and terrorist financing and the size of our business. We shall ensure that the employees taking up such key positions are suitable and competent to perform their duties

The HR Department is instructed to verify the identity, cross check all the references, family background and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.

The department should obtain the following documents:

- 1 Photographs
- 2 Proof of address
- 3 Identity proof
- 4 Proof of Educational Qualification
- 5 Proof of Bank Account Details

15. Training of staff/Employees

All the staff members involved in front office dealings, back office, KYC & Compliances, Risk Management or any kind of client dealings (including the APs and their dealing staff) need to be adequately trained in AML and CFT (Combating Financing of Terrorism) procedures. They should fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of our systems being misused by unscrupulous elements.

Accordingly, we have an ongoing employee-training programme (in-house as well as sending employees for attending of independent training workshops) so that the concerned staff are adequately trained in AML and CFT procedures. These training programs are conducted on periodic basis and each of the concerned staff is required to attend at least 2 such training programs each year.

Further, the Principle Officer is authorized to ensure that all the concerned staff is well versed with latest modifications in the PMLA policy framework and is adequately sensitized to the risks of ML & TF.

16. Investor' Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have 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 clients with regard to the

motive and purpose of collecting such information. We, therefore need to sensitize prospective client that these requirements emanating from AML and CFT framework.

This may either be done by preparing specific literature or by educating the clients/sub-brokers/Authorised Person on the objectives of the Anti Money Laundering (AML) / Combating Financing of Terrorism (CFT) programme.

17. Review of PMLA/CFT Procedures

The policy shall be reviewed annually so as to incorporate the latest change(s) in the Anti Money Laundering Act 2002 or change in any other act, bye-laws, rules, regulations of SEBI, CBI or in any statutory and regulatory government department related to or affect to this.

Further the review of this policy framework shall be undertaken by the person other than the one who has framed this policy.

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

“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(https://www.sebi.gov.in/sebi_data/commdocs/jun-2023/Annexure-1_Government_Order_dated-February_02,2021_p.pdf) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 https://www.sebi.gov.in/sebi_data/commdocs/jun-2023/Annexure-2_Gazette_notification_dated-June_08,2021_p.pdf). A corrigendum dated March 15, 2023 and April 22, 2024 has also been issued in this regard (https://www.sebi.gov.in/sebi_data/commdocs/jun-2023/Annexure-3_Corrigendum_Order_dated-March_15,2023_under_UAPA_p.pdf) and Annex 4 Designation of Central Nodal officer MHA Corrigendum April 22, 2024_p.pdf (sebi.gov.in) . The list of Nodal Officers for UAPA is available on the website of MHA”. In terms of said regulations, we as an intermediary have to ensure that we 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).

19. 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

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.

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."

We Shall-

- (i) Maintain the list of individuals/ entities ("Designated List") and update it, time to time without any 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, we 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) 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, we 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, without delay, mentioned in paragraphs (ii) and (iii) above, 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 (ii) and (iii) above.

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.

We shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts.

19. Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, we 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>

We shall carefully go through all the reporting requirement ([https://www.sebi.gov.in/sebi_data/-commondocs/jun-2024/Brochures on FIU_p.pdf](https://www.sebi.gov.in/sebi_data/-commondocs/jun-2024/Brochures%20on%20FIU_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](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, we 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, if any.
- 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 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.

We shall not put any restrictions on operations in the accounts where an STR has been made. We and our 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. Confidentiality requirement does not inhibit information sharing among entities in the group.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, we 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.

Lists of Red Flag Indicators for Terrorist Financing – FIU

- a. Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- b. Management appears to be acting according to instructions of unknown or inappropriate person(s). Unnecessarily complex client structure.
- c. The client is reluctant to provide all the relevant information or the accountant has reasonable doubt that the provided information is correct or sufficient.
- d. Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.

- e. Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
- f. Client starts or develops an enterprise with unexpected profile or early results. Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
- g. Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- h. Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
- i. Large international payments with no business rationale. Unusual financial transactions with unknown source.
- j. Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.

RED FLAG INDICATORS FOR TERRORIST FINANCING BY FIUS OF OTHER COUNTRIES

A. Financial and behavioural Indicators Published by The Egmont Group of Financial Intelligence Units

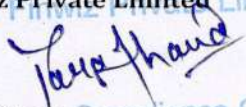
Indicators linked to the financial transactions:

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
4. Transactions which are inconsistent with the account's normal activity.
5. Multiple cash deposits and withdrawals with suspicious references.
6. No business rationale or economic justification for the transaction.

Behavioural Indicators:

1. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.
3. Inclusion of the individual in the United Nations 1267 Sanctions list.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family member or third party accounts.
7. Use of false identification.
8. Abuse of non-profit organization.

For CNB Finwiz Private Limited Limited


Compliance Officer Compliance Officer