

Anti-Money Laundering Policy and Procedures

FOUR DIMENSIONS SECURITIES (INDIA) LIMITED

Periodicity of Review: As and when changes occurs / Yearly	Last reviewed on: 13-02-2024
Office responsible for implementation: Compliance Officer	

ANTIMONEY LAUNDERING POLICY & PROCEDURES

01. Introduction

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified there under came into force with effect from July 1, 2005. Section 12 of PMLA, inter-alia, requires all intermediaries associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 to maintain a record of all transactions, the nature and value of which has been prescribed under the rules notified under the PMLA. Pursuant to this, Securities and Exchange Board of India (SEBI) issued Guidelines on Anti Money Laundering Standards and various circulars from time to time to implement the provisions of PMLA in the securities market and to prevent and impede money-laundering and combat financing of terrorism. **Four Dimensions Securities (India) Limited** (hereinafter referred to as 'FDSIL' or 'the Company'), hereby adopts and bring into effect this **Anti Money Laundering Policy & Procedures** (AML Policy & Procedures) in accordance with the provisions of PMLA and the rules made thereunder, SEBI Guidelines and Circulars issued from time to time on this subject. The policy applies not only to money laundering, but also to terrorist financing. All references to money-laundering in this policy, company policies and procedures and standards include terrorist financing as appropriate.

02. Objectives

The objectives of this Policy are to:

- Prevent and deter the use of the Company/Company's services by money launderers or those involved in criminal activities including financing of terrorism and to protect the reputation of the Company.
- Protect the Company and its employees against unfounded allegations of facilitating money laundering and terrorist financing; and
- Protect the Company and its employees against any criminal, civil and regulatory actions which might result from inadvertent involvement in money laundering and/or terrorist financing or from failure in operational controls.

03. Definitions:

In this Act, unless the context otherwise requires,—

- "Act" means the Prevention of Money-laundering Act, 2002 (15 of 2003);
 - "Central KYC Records Registry" means a reporting entity, substantially owned and controlled by the Central Government, and authorised by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client as referred to in clause (ha) in such manner and to perform such other functions as may be required under these rules:
 - "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 Act;
 - "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 -;
 - the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
 - the managing partner if the reporting entry is a partnership firm,
 - the proprietor if the reporting entity is a proprietorship concern,
 - the managing trustee if the reporting entity is a trust
-

- 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
- 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.

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

- “Designated Officer” means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts.
- “Director” or “Additional Director” or “Joint Director” means a Director or Additional Director or Joint Director, as the case may be, appointed under sub-section (1) of section 49;
- “intermediary” means,—
 - a stock-broker, sub-broker share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); or
 - an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 (74 of 1952) or any member of such association; or
 - intermediary registered by the Pension Fund Regulatory and Development Authority; or
 - a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);
- “person” includes;—
 - an individual,
 - a Hindu undivided family,
 - a company,
 - a firm,
 - an association of persons or a body of individuals, whether incorporated or not,
 - every artificial juridical person, not falling within any of the preceding sub-clauses, and
 - any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses;
- "Principal Officer " means an officer designated by a reporting entity;
- "Regulator " means a person or an authority or a Government which is vested with the power to license, authorise, register, regulate or supervise the activity of reporting entities or the Director as may be notified by the Government for a specific reporting entity or a class of reporting entities or for a specific purpose;
- "Rules " means the Prevention of Money-laundering (Maintenance of Records) Rules, 2005;

All other words and expressions used and not defined in these rules but defined in the Act shall have the meaning respectively assigned to them in the Act.

04. Designation of the Officers for ensuring Compliance with provisions of PMLA and their responsibilities:

Principal Officer:

Mr Chirag Doshi has been appointed as the principal Officer of the Company.

The following are the responsibilities of the Principal Officer:

- To ensure compliance with the provisions of the PMLA and this AML Policy & Procedures.
-

- Furnish information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with FDSIL;
- Identify and assess potentially suspicious transaction.

The Principal Officer shall have unrestricted access to the Company's Offices, IT Systems and records in order to carry out his responsibilities.

Designated Director:

Mr. Sandeep Kejariwal has been appointed as the Designated Director of the Company.

The above mentioned officers are appointed as per the provisions of PMLA till such time SEBI, Stock Exchanges and Depositories identifies an official to act as such.

FDSIL shall immediately intimate the name, designation and address including email address of the Designated Director and the Principal Officer to the Director.- Any change in the particulars of Principal Officer shall also be immediately intimated to the Office of the Director-FIU and the Stock Exchanges.

05. Detailed Directives

A. Client Due Diligence:

The Company shall put in place appropriate customer due diligence measures, which should be applied to all customers (new as well as existing). These measures comprise:

The Directives has the following Key Elements:

- Client Identification Policy (CIP)
- Client's Acceptance Policy
- Risk Profiling of Clients;
- Clients of Special Category (CSC);
- Reliance on Third Party for Client Due Diligence; and
- Continuous Monitoring of Transactions & Identification of Suspicious Transactions/Activities

(a) Client Identification Policy:

- (i) Before admitting any person as a client, the Company shall obtain sufficient information in order to identify the customer and any other person(s) with whom lies the beneficial ownership or ultimate control. The Beneficial owner is the natural person or person who ultimately own, control or influence a client and / or person on whose behalf a transaction is been conducted. The same should be done for all the existing customers as well. This should be done by obtaining 'Know Your Customer' (KYC) information;
 - (ii) A list of the nature and type of documents/information that may be relied upon for client identification is given in the Annexure - A. Officials have to follow these guidelines based on their experience of dealing with such persons/entities, normal prudence and the legal requirements as prescribed here and as amended from time to time by regulators and laws.
 - (iii) KYC information should be updated on a regular basis during the course of business relationship;
-

- (iv) The customer should be identified by the Company using documents/information from reliable sources. Adequate information to satisfactorily establish the identity of each client and the purpose of the intended nature of the relationship should be obtained by the Company;
- (v) Understand the ownership and control structure of the client;
- (vi) Due Diligence measures shall be reviewed when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts pertaining the adequacy or veracity of previously obtained data.

Beneficial Owner:

- **For clients other than individuals or trusts:**

Where the client is a person *other than an individual or trust*, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

- a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest. Explanation: Controlling ownership interest means ownership of / entitlement to:
 - i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
 - ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
 - iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.
- b. In cases where there exists doubt under clause (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means. Explanation : Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner;
- c. Where no natural person is identified under clauses (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

- **For client which is a trust:**

- a. Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% 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.

- **Exemption in case of listed companies:**

- a. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not
-

necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

- **Applicability for foreign investors:**

- a. Intermediaries dealing with foreign investors' viz., Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued vide SEBI circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and amendments thereon, for the purpose of identification of beneficial ownership of the client.

(b) Clients Acceptance Policy:

The Company has developed client acceptance policy and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. Staff should adhere to following safeguards while accepting customers:

- Customers who are acceptable to Company as per the Risk categorization should fulfill all criteria related to submission of Officially Valid Documents (OVD) as defined by the SEBI, RBI, Exchanges, Depositories, etc from time to time
- No Trading account should be opened in a fictitious/benami name or on an anonymous basis, or in the name of a suspended/banned entity;
- Company shall refrain from entering into any transactions where Company is unable to apply appropriate Client Due Diligence (CDD) measures.
- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in gambling activities.
- In the event, the customer is permitted to act on behalf of another person/entity, Company shall verify that the client has the necessary authority to do so by scrutinizing the authorizing document/s.
- Before opening an account it must be ensured that the identity of the prospective client does not match with a person having known criminal background and that there are no prohibitory orders/sanctions against the prospective client by any enforcement/regulatory agency or the proposed client is not banned from trading in Stock Market(s)
- Before accepting any person as a client and at regular interval, it must be ensured that such person's name does not appear and is not linked in any way to the individuals and entities listed in the consolidated list available on the UN website at: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml; <http://www.un.org/sc/committees/1988/list.shtml>.. The Company shall intimate full details of accounts bearing resemblance to any of the individuals/entities in the aforesaid consolidated list to SEBI and FIU-IND;

Company shall determine if the existing or potential client is a Politically Exposed Person (PEP) by seeking additional information from clients, accessing publicly available information etc. If the existing/potential client is found to be PEP, approval should be obtained from the Whole-time Director of the Company to admit the PEP as client or to continue the existing business relationship. The Company shall also seek the details of source of funds of clients identified as PEP;

It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation should not become too restrictive and must not result in denial of the company's services to general public.

(c) Risk Profiling of Clients:

- (i) Risk Profiling is based on client's identity, social/ financial status, nature of business activity and information about client's business and their location. Based on the risk profiling clients should be grouped into the following three categories –

	Low Risk Clients	Medium Risk Clients	High Risk Clients
Definition	<p>a. Corporates with the respectable Social and Financial Standing;</p> <p>b. Clients like salaried people – wherein all their income and expenses details are transparent and well structured.</p>	<p>a. Clients those are less risky in nature as compare to high risk customers – can be categorised as Medium Risk.</p> <p>b. Where the Trading and settlement pattern of the client is suspicious;</p> <p>c. Intraday client or speculative client.</p>	<p>a. Clients are categorized as Higher Risk clients depending on client's background, nature and location of activity, country of origin, sources of funds and his client's profile, etc.;</p> <p>b. Clients who have defaulted in the past;</p> <p>c. Clients who have a suspicious background;</p> <p>d. High Net-worth (above 2500 crores) Clients and whose identity and source of wealth are difficult to identify;</p> <p>e. PEP, Clients of Special category, Dormant Account.</p>

- (ii) The Company shall apply Clients due diligence measures to clients on a risk sensitive basis i.e. applicability of client identification procedures, documentary requirements, ongoing account monitoring, transaction monitoring & risk management will depend on the risk profile of customer. Client identified as high risk category shall be subjected to enhanced client due diligence process. Conversely, a simplified due diligence process may be adopted for low risk categories of customers.
- (iii) In certain limited circumstances, within the overall framework of the SEBI guidelines, the Company may apply reduced or simplified Customer Due Diligence measures for certain types of customers, products or transactions, taking into account all the risk factors. Any such reduced customer due diligence procedures must be approved by the Principal Officer.

(d) Clients of Special Category (CSC):

Customers who may pose a particular risk to the Company, to money laundering deterrence programme and to the Company's reputation, and who should normally be treated as high risk and subject to enhanced customer due diligence, include, but are not limited to the following:

- Customers with complex account relationships e.g. multiple accounts in one;
- Non-Resident Clients;
- High Net-worth Clients;
- Trust, Charities, NGOs and organizations receiving donations;
- Companies having close family shareholdings or beneficial ownership;
- Politically Exposed Person (PEP):

- Current/Former Head of State, current or former Senior High-Profile politicians and connected persons;
- Companies offering foreign exchange offerings;
- Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, 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, etc. We shall also independently access and consider other publicly available information along with any other information which we may have access to;
- Non face to face clients;
- Clients with dubious reputation as per public information available etc.

For clients other than as specified under Client of Special Category (CSC), we are defining risk categorization of clients in Low, Medium & High Risk based on their trading pattern, Financials etc. & were reviewed periodically. The Company shall not be restrictive to the list illustrated above and may ascertain CSC classification.

(e) Reliance on Third Party for Client Due Diligence:

The Company may rely on the third party for the purpose of:

- a. Identification and verification of the Identity of the Client, and
- b. Determination of whether a client is acting on behalf of a beneficial owner, and 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 obligation under the PML Act;

Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PMLA Rules and shall be in accordance with the regulations and circulars/guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable;

(f) Continuous Monitoring of Transactions & Identification of Suspicious Transactions/Activities:

- (i) The Company shall undertake appropriate scrutiny and monitoring of client's account activity and transactions on an ongoing basis in order to identify any unusual and potentially suspicious activity. This is possible only when the Company's staff has an understanding of the normal activity of the client so that they can identify any deviant transactions/activities;
 - (ii) Transactions and account activity involving customers categorized as high risk should be subject to enhanced monitoring. The monitoring of transaction will also be done on the basis of volume of trading done by the client in proportion to his financial details / networth as disclosed in the KYC. The financial details will also be updated on periodical basis to have a proper control on their transactions;
-

B. Maintaining & Retaining Records

- i. The Company shall ensure compliance with the record keeping requirement contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant Legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

Adequate records of all transactions should be maintained in order to permit reconstruction of transactions including the amounts, types of currency involved, the origin of funds received into client's accounts and the beneficiaries of payments out of client's accounts so as to provide, if necessary, evidence for prosecution of criminal behavior.

- ii. The Company shall maintain record of following transactions as prescribed under Rule 3, notified under the PMLA:
 - a. all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;
 - b. all series of cash transactions integrally connected to each other which have been valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10 lakh;
 - c. all transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency;
 - d. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions;
 - e. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules;
 - f. all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
 - g. all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be
- iii. For the above transactions, Company shall also maintain following information:
 - a. the nature of the transactions;
 - b. the amount of the transaction and the currency in which it is denominated;
 - c. the date on which the transaction was conducted; and
 - d. the parties to the transaction.
- iv. The company shall maintain and preserve the 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 have to be recorded for a period of five years from the date of transactions between the client and intermediary. However as per Regulation 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 & SEBI/HO/MRD/DDAP/CIR/P/2020/153 dated August 18th 2020, all records evidencing the identity of its clients and beneficial owners as well as the account files and business correspondence shall be maintained and preserved for a period of 8 years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later;
- v. In situations where the records relate to on-going investigations 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;

- vi. Further, the records mentioned in Rule 3 of PMLA Rules and the information reported to the Director, Financial Intelligence Unit – India as required under Rule 7 and 8 of the PMLA Rules, have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary;
- vii. The record of the transactions is preserved and maintained in term of Section 12 of the PMLA and that transaction of a suspicious nature or any other transaction 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.

C. Monitoring and Reporting of Suspicious Transactions

- i. “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 the proceeds of crime;
or
 - b) appears to be made in circumstances of unusual or unjustified complexity; or
 - c) appears to have no economic rationale or bonafide purpose;
 - d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
 - ii. Some of the circumstances which may lead to suspicion and certain transactions which are deemed to be suspicious in nature are:
 - False identification documents or identification documents which could not be verified within reasonable time;
 - Non-face to face clients;
 - Doubt over the real beneficiary of the account;
 - Accounts opened with names very close to other established business entities;
 - Suspicious background or links with known criminals;
 - Receipt back of welcome kit undelivered at the address given by the client;
 - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale;
 - Unexplained transfers between multiple accounts with no rationale;
 - Unusual activity compared to past transactions;
 - Use of different accounts by client alternatively;
 - Sudden activity in dormant accounts;
 - Activity inconsistent with what would be expected from declared business;
 - Account used for circular trading;
 - Unusual or unjustified complexity in transactions;
 - No economic rationale or bonafide purpose of transactions;
 - Doubtful source of funds;
 - Transfer of investment proceeds to a 3rd party;
 - Transactions reflecting likely market manipulations;
 - Suspicious off-market transactions;
 - Transaction value just below threshold in an apparent attempt to avoid reporting;
 - Large sums being transferred from overseas for making payments;
 - Transactions inconsistent with the clients apparent financial standing;
 - Inconsistency in the payment pattern by client;
 - Bulk deal which is not at market price or prices appear to be artificially inflated/deflated;
-

- Cash transaction with customers;
 - Unusual transactions by Clients of Special Category (CSC), businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export and import;
 - Transactions in securities could be considered as suspicious if they are far away from the prevailing market price or theoretical market price and are accompanied with offsetting transactions without satisfactory explanations;
 - Transactions of a client would be considered as suspicious if the client does not confirm the transactions, does not sign the ledger account confirmations, securities ledger confirmations or does not effect receipts or payments of moneys due for a considerably long period of time without satisfactory explanations;
 - Clients with no discernible reason for using Company's services e.g. clients with distant addresses who could find the same service nearer home or client's requirements not in the normal pattern of Company's business which could more easily be serviced locally;
 - "Cold calls" by investors who are not known personally by the staff member or the market in general;
 - Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active, or the investor's business;
 - Buying and selling of securities with no discernible purpose or in unusual circumstances e.g. churning at the client's request;
 - Large quantity or frequent buying & selling by clients in scrips categorized as 'Trade for Trade' by Exchange;
 - Large numbers of transactions of small amounts by the same client in the same security, first purchased and then sold, the proceeds being credited to an account different from the original account;
 - Transactions not in keeping with normal practice in the market to which it relates, i.e. with reference to market size and frequency or at off-market prices;
- iii. All staff members shall ensure that any transaction and/or activity which is believed to be suspicious is reported to the Principal Officer who shall validate whether the transaction/activity is of suspicious nature or not. However, it should be ensured that there is no discontinuity in dealing with the client until told otherwise and the client should 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 or other action taken. Such customer's accounts should be reviewed in conjunction with the Principal Officer and a decision should be made as to whether it should be closed;
- iv. In some cases, customers may abandon transactions on being asked to give some additional details/documents/information. It is clarified that staff shall report all such attempted transactions in Suspicious Transactions Report, even if they are not executed by customers, irrespective of the amount of the transaction.
- v. The compliance department of the Company shall randomly examine a selection of transactions undertaken by clients to examine and comment on whether or not they are in the nature of suspicious transactions.

D. Procedure for freezing & unfreezing of funds, financial assets or economic resources or related services:

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the prevention of, and coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government had issued an Order dated March 14, 2019 detailing the procedure for the implementation of Section 51A of the UAPA, in view of the

reorganization of Divisions in the Ministry of Home Affairs and allocation of work relating to countering of terror financing to the **Counter Terrorism and Counter Radicalization (CTCR)** Division.

Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The obligations to be followed by intermediaries to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Master Circular ref. no: SEBI/ HO/ MIRSD/ MIRSD-SEC-5/P/CIR/ 2023/022 dated February 03, 2023, which needs to be complied with scrupulously. Accordingly, in order to ensure compliance with the Order the company shall follow the following procedure:

In case if any client is found to be guilty under the PMLA provisions then the following procedure to be followed by the Company, will be as under:

1. If the particulars of any of customer/s match the particulars of designated individuals / entities, the Company shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on their books to the Central Nodal Officer UAPA, at Fax No.011-23092551 and also convey over telephone on 011-23092548. The Company would also convey the information through e-mail at jsctcr-mah@gov.in;
2. The Company would inform the UAPA Nodal Officer of State/UT so that they may take effective action like informing the State Police and / or the Central Agencies for conducting the verification of the individuals / entities identified by the registered intermediaries;
3. The Company to provide full support to the appointed agency for conducting of the verification so that the verification get completed within a period of 5 working days;
4. The Company would not provide any prior notice to the designated individuals / entities.

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

- i. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the stock exchange/ depositories and UAPA Nodal Officer of State / UT;
 - ii. The Stock exchanges / depositories and registered intermediaries shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS – I Division of MHA as per the contact details given in Annexure of the SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 circular dated February 03, 2023 within two working days;
 - iii. The Central Nodal Officer for UAPA,, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall
-

pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock broker, depositories and registered intermediaries. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the Central Nodal officer of shall inform the applicant.

06. Reporting to Financial Intelligence Unit – India:

- All other requirements under FATCA/PML/FIU-Ind relating to appointment of designated officer/director, principal officer and reporting requirements relating to filling of Suspicious Transaction Report (STR), Cash Transaction Report (CTR), counterfeit currency report (CCR) and other applicable reports filling under FATCA will be complied with in terms of the direction of the Regulatory authorities to the extent applicable to Company;
- Principal Officer of the Company shall submit Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) as prescribed under PMLA Rules to:

**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

and shall adhere to the instructions, guidelines, formats, files and data as provided on the website of FIU – IND while reporting and shall also adhere to the following:

a. Cash Transaction Reports (CTRs):

- The CTRs (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month;
- The Company shall submit the CTRs in Electronic format;
- It should be accompanied by summary of CTR in physical form duly signed by the Principal Officer.

b. Suspicious Transaction Reports (STRs):

- All suspicious transactions shall be reported by the Principal Officer to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion;
- The Principal officer shall submit the STRs in Electronic format

c. The Principal Officer will be responsible for timely submission of CTRs and STRs to FIU-IND;

d. Utmost confidentiality should be maintained in filing of CTRs and STRs to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

- e. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

Every control system should be established in the organization to take care that the reporting of suspicious activity should be done to the regulators only and no client should be informed to the suspicious reporting being done a but themselves or about anybody else. The Company and its staff are strictly required to ensure that there is no 'tipping-off' to any customers about any suspicious transaction reporting that has been made to the regulators. The organization may use the learning from the suspicious activity to train the staff for controlling any suspicious activity and use the information for investor / clients awareness about the suspicious transactions.

07. Co-operation with Authorities

- (i) The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining customer confidentiality. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.
- (ii) The Company and its staff shall strictly ensure that there is no 'tipping-off' to customers about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a customer, it may seriously hamper the enquiry/investigation of the authorities.
- (iii) There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

08. Hiring of Employees:

The company has a sufficient system of screening the employees before their appointment so that they are suitable and competent to perform their duties. The company would also carry out on going employee training programme so that the Employees are adequately trained in AML and CFT procedures as required.

The HR department will also be carrying out the background check of the employee being hired by calling the references provided by the employee or a third party verifier agency to carry out a proper check before employing the employee. The HR department will also try to get the creditability of the employee by talking to the previous employers and get their feedback of the senior / HR department / the department where the employee was working with his past employments.

09. Training:

- (i) There shall have an ongoing employee training program conducted by Principal Officer or Senior Management of the Company.
 - (ii) Participation of all the Key Employees in the Seminars conducted by various Regulatory bodies from time to time, so that the members of the staff are adequately trained in AML and CFT procedures.
-

- (iii) All the Circulars issued by various Regulatory bodies including that of PMLA, are circulated to all the key employees and the same are also being discussed in length, in the Training Program.
- (iv) Training program shall have special emphasis on 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.
- (v) The training of the staff includes but not limited to following Agenda:
 - How to identify red flags and signs of money laundering that arise during the course of the employees duties;
 - what to do once the risk is identified;
 - what employees' roles are in the firm's compliance efforts and how to perform them; and
 - the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

10. Investor Education:

The company also intends to take effective steps for Investor Education regarding the PMLA regulations. Accordingly the KYC team of the company intends to Educate the Investor regarding the requirements of PMLA and will also call for various information like Income proof / DP holding /Networth, etc. so as to understand the financial position of the client.

11. Monitoring and Review of the Company's AML Policy & Procedures:

- (i) The Company shall undertake regular monitoring of its operations through line management and/or Compliance to check that all businesses are complying with the Company's AML Policy& Procedures as well as local legal and regulatory requirements as prescribed under the PMLA and by SEBI.
- (ii) Operational and functional review work shall be undertaken by Compliance and/or Audit functions, as appropriate. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review programme and responsibility.
- (iii) The level and frequency of monitoring and review work shall be undertaken having regard to materiality and risk in relation to the business and customer base.

This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

12. Further Information:

Any queries or doubts concerning Company AML Policy& Procedures or any local legislation or regulation or Circulars or Guidelines relating to Anti Money Laundering and/or Combating Financing of Terrorism shall be referred to the Principal Officer of the Company.

13. Approval Authority:

This policy shall be approved by the Board of Directors.

Annexure -A

Customer Identification Procedure

Documents that may be obtained from customers

Customers	Documents (Certified copy of any one of the following officially valid document)
Accounts of individuals	<p>Identity Proof: (Copy of one of the following)</p> <ul style="list-style-type: none">(i) Passport(ii) PAN card(iii) Voter's Identity Card issued by Election Commission(iv) Driving License(v) Aadhar Card <p>Residence proof: (Copy of one of the following)</p> <ul style="list-style-type: none">• Utility Bill (Latest Telephone / Post-paid mobile / Electricity bill)• Property or Municipal Tax receipt• Bank Account or post office savings bank account statement• Passport• Driving Licence• Voter's Identity Card• Aadhar Card. <p>A copy of the marriage certificate or Gazette notification, in case of change in name</p>
In case of Non-Individual (As applicable)	<p>Identity & Residence proof (Copies of the following)</p> <ul style="list-style-type: none">• Income Tax PAN Card• Incorporation Certificate & Memorandum & Articles of Association (Registration Certificate & Deed, in case of Partnership firm/Trust)• CST/VAT/Service Tax registration /GST registration/ Shops & Establishment Certificate, as applicable• List of Directors/Partners/Trustees along with their OVDs as above.• Latest shareholding pattern, along with the list of major shareholders having more than 25% of holding, in case of company.• Utility bill